PLANET
Networking & Communication

802.11g Wireless MIMO Broadband Router

WMRT-414

User's Manual

Copyright

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution:

To assure continued compliance.(example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm(8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8,2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

WEEE regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

User’s Manual for PLANET 802.11g Wireless MIMO Router

Model: WMRT-414

Rev: 1.0 (December. 2005)

Part No. EM-WMRT414

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION..1

1.1 PACKAGE CONTENTS 1

1. 2 FEATURES 1

1.3 SPECIFICATION..2

CHAPTER 2 HARDWARE INSTALLATION......................................3

2.1 HARDWARE CONNECTION..3

2.2 LED INDICATORS..4

CHAPTER 3 WEB LOGIN 5

CHAPTER 4 QUICK SETUP 7

4.1 TIME ZONE 7

4.2 BROADBAND TYPE 8

4.2.1 Cable Modem..9

4.2.2 Fixed-IP xDSL 10

4.2.3 PPPoE xDSL 11

4.2.4 PPTP xDSL..12

4.2.5 L2TP xDSL 14

4.2.6 Telstra Big Pond 16

4.2.7 Save Settings Successfully..16

CHAPTER 5 GENERAL SETUP 18

5.1 SYSTEM..19

5.1.1 Time Zone 20

5.1.2 Password Setup..21

5.1.3 Remote Management 22

5.2 WAN..23

5.2.1 Dynamic IP..24

5.2.2 Static IP 25

5.2.3 PPPoE 26

5.2.4 PPTP..27

5.2.5 L2TP 28

5.2.6 Telstra Big Pond 29

5.2.7 DNS 30

5.2.8 DDNS..31

5.3 LAN..32

5.4 WIRELESS 33

5.4.1 Basic Settings 34

5.4.2 Advance Settings 34

5.4.3 Security 35

5.4.4 Access Control 41

5.5 QoS 42

5.5.1 Add/Edit QoS Rule 43

5.6 NAT 44

5.6.1 Port Forwarding 45

5.6.2 Virtual Server 46

5.6.3 Special Applications 48

5.6.4 UPnP 50

5.6.5 ALG Settings 51

5.7 Firewall 51

5.7.1 Access Control 53

5.7.2 URL Blocking 55

5.7.3 DoS 56

5.7.4 DMZ 57

CHAPTER 6 WIRELESS CONFIGURATION 59

6.1 AP Mode 59

6.2 AP Bridge - Point to Point Mode 61

6.3 AP Bridge - Point to Multipoint Mode 62

6.4 AP Bridge - WDS Mode 63

6.5 Security setting of bridge mode 64

6.5.1 WEP 65

6.5.2 WPA-PSK 66

CHAPTER 7 STATUS 67

7.1 Internet Connection 68

7.2 Device Status 68

7.3 System Log 69

7.4 Security Log 70

7.5 Active DHCP Client 71

7.6 Statistics 72

CHAPTER 8 TOOLS 73

8.1 Configuration Tools 73

8.2 Firmware Upgrade 74

8.3 Reset 75

APPENDIX A NETWORK ADAPTER INFORMATION 77

APPENDIX B FREQUENTLY ASK QUESTION......................78

APPENDIX C GLOSSARY 80

Chapter 1 Introduction

Thank you for purchasing WMRT-414. This manual guides you on how to install and properly use the WMRT-414 in order to take full advantage of its features.

1.1 Package Contents

Make sure that you have the following items:

- One WMRT-414
- One AC Power Adapter
- One User's Manual CD
- One Quick Installation Guide
- Three External Dipole Antenna

Note:	If any of the above items are missing, contact your supplier for support.

1. 2 Features

- Compliant with 802.11g / 802.11b standard
- Farther coverage, less dead spaces and higher throughput with MIMO technology
- Supports Turbo Mode to enhance the data transfer speed within the specific wireless network (the wireless client adapter must support Turbo mode as well)
- Supports WMM (WiFi Multi-Media) function to meet the multi-media data bandwidth requirement (the wireless client adapter and the application must support WMM as well)
- Allow multiple users to share a single Internet connection
- Internet Access via Cable or xDSL modem
- Supports 64/128-bit WEP, WPA (TKIP with IEEE 802.1x), WPA2 (AES with IEEE 802.1x) functions for high level of security
- Access Private LAN Servers from the Public Network
- AP / WDS / Bridge modes supported
- Equipped with four LAN ports (10/100M) and one WAN port (10/100M), Auto-MDI/MDI-X supported
- Support DHCP Server for easy setup
- System status monitoring including Active DHCP Client, Security Log and Device/Connection Status
- Easy to use Web-based GUI for configuration and management purposes
- Remote Management allows configuration and upgrades from a remote site (over the Internet)
- DHCP/PPPoE/PPTP/L2TP/Fixed IP allocation
- MAC/IP filter access control, URL blocking
- SPI firewall + DoS prevention protection
- Support UPnP function

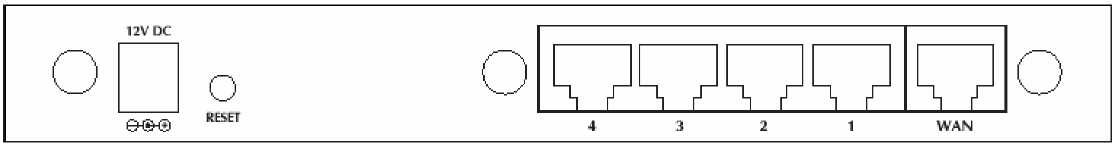
1.3 Specification

Standard	IEEE 802.11g/802.11b with MIMO technology
Signal Type	DSSS (Direct Sequence Spread Spectrum)
Modulation	OFDM/ QPSK / BPSK / CCK
WAN Port	1 x 10/100Base-TX, Auto-MDI/MDI-X
LAN Port	4 x 10/100Base-TX, Auto-MDI/MDI-X
Antenna connector	3 x RP-SMA connectors
Data Encryption	64 bit / 128 bit WEP, WPA-PSK, WPA, WPA2
Frequency	2.4GHz - 2.484GHz
Data Rate	Up to 54Mbps (with automatic scale back)
LED Indicators	PWR, WLAN LAN: LNK/ACT * 4, 10/100Mbps * 4 WAN: LNK/ACT * 1, 10/100Mbps * 1
Power Requirement	12V DC, 1A
Power Consumption	TX power consumption: <650mA RX power consumption <350mA
Temperature	Operating :0 ~ 40 degree C Storage: -20 ~ 70 degree C
Humidity	Operating: 0 ~ 90% Storage: 0 ~ 95% Non-Condensing
Dimensions	190 x 98 x 35 mm
Weight	355g
Output Power	18dBm±2dBm

Chapter 2 Hardware Installation

Before you proceed with the installation, it is necessary that you have enough information about the WMRT-414.

2.1 Hardware Connection

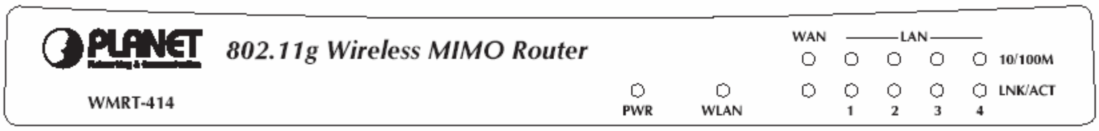


1. **Locate an optimum location for the WMRT-414.** The best place for your WMRT-414 is usually at the center of your wireless network, with line of sight to all of your mobile stations.
2. **Adjust the antennas of WMRT-414.** Try to adjust them to a position that can best cover your wireless network. The antenna's position will enhance the receiving sensitivity.
3. **Connect RJ-45 cable to WMRT-414 LAN port.** Connect one of the LAN ports on WMRT-414 to your LAN switch/hub or a computer with a RJ-45 cable.
4. **Connect RJ-45 cable to WMRT-414 WAN port.** Connect xDSL/Cable Modem to the WAN port on WMRT-414. Usually, this cable would be provided with your modem. If no cable was supplied with your modem, please use a RJ-45 Ethernet cable
5. **Plug in power adapter and connect to power source**. After power on, WMRT-414 will start to operate.

Note: ONLY use the power adapter supplied with the WMRT-414. Otherwise, the product may be damaged.
If you want to reset WMRT-414 to default settings, press and hold the **RESET** button over 10 seconds and release. And then wait for WMRT-414 restart.

RESET Button	This button has two functions: **To Reboot machine without Clearing Existing Configurations:** Press the reset button with a pencil tip (for less than 5 seconds), machine will re-boot itself, the existing configurations will be kept. **To Clear All Data and restore the factory default values:** Press the reset button for longer than 10 seconds and the router will reset itself to the factory default settings (warning: your original configurations will be replaced with the factory default settings)

2.2 LED Indicators

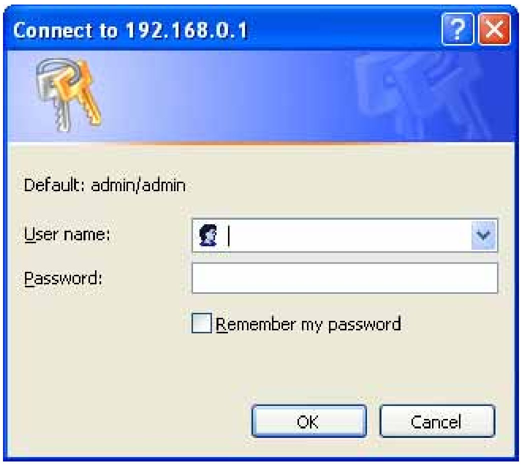


LED		Color	STATE	MEANING
PWR		Green	On	Device power on
			Off	Device power off
			Blinking	During boot up procedure
WLAN		Orange	Blinking	Transmitting or receiving data through the Wireless LAN
			Off	Wireless LAN is no function
WAN	**10/100M**	Green	On	WAN port is connected at 100Mbps
			Off	WAN port is connected at 10Mbps
	LNK/ACT	Green	On	Link is established
			Blinking	Packets are transmitting or receiving
LAN	**10/100M**	Green	On	LAN is connected to 100Mbps device
			Off	LAN is connected to 10Mbps device
	LNK/ACT	Green	On	Link is established
			Blinking	Packets are transmitting or receiving
			Off	LAN port is not connected

Chapter 3 Web Login

A WMRT-414 with an assigned IP address allows you to monitor and configure via web browser (e.g., MS Internet Explorer or Netscape).

1. Open your web browser.
2. Enter the IP address of your WMRT-414 in the address field (default IP address is http://192.168.0.1).
3. A User Name and Password dialog box will appear. Please enter your User Name and Password here. Default User Name and Password are both “admin”. Click OK.


Connect to 192.168.0.1

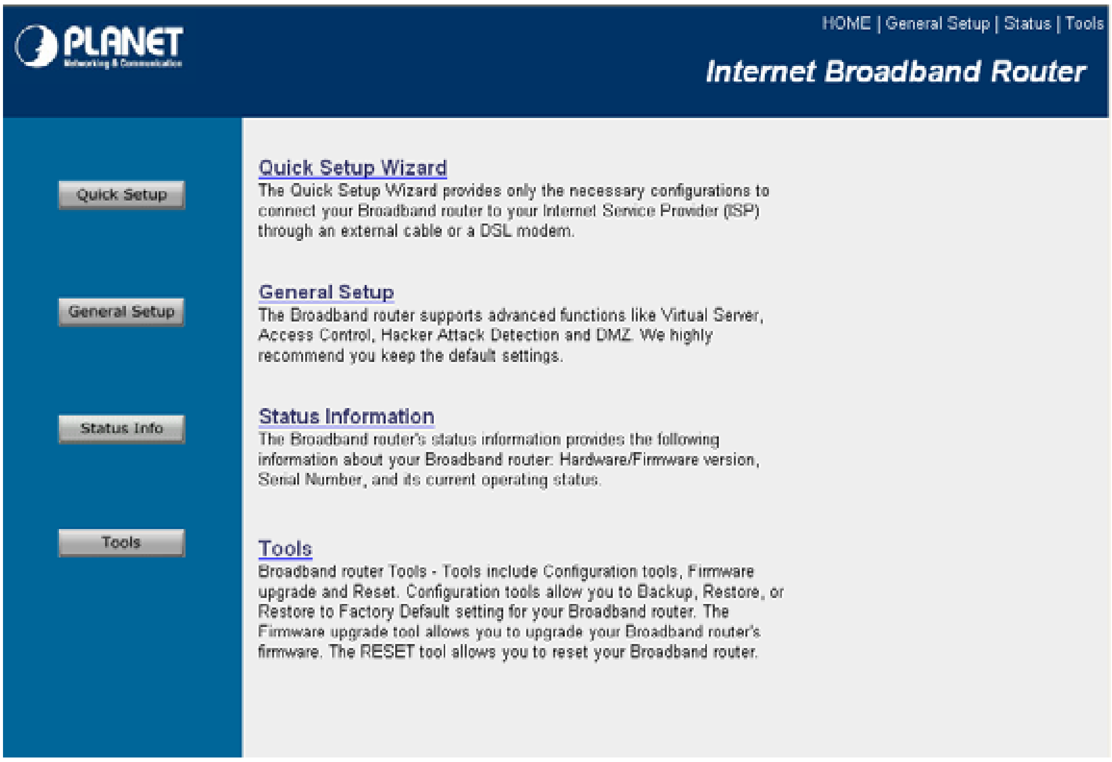
Default: admin/admin

User name:

Password:

□ Remember my password

4. Then you will see the WMRT-414 HOME screen as below.


PLANET
HOME | General Setup | Status | Tools
Internet Broadband Router
Quick Setup
General Setup
Status Info
Tools

Quick Setup Wizard
The Quick Setup Wizard provides only the necessary configurations to connect your Broadband router to your Internet Service Provider (ISP) through an external cable or a DSL modem.

General Setup
The Broadband router supports advanced functions like Virtual Server, Access Control, Hacker Attack Detection and DMZ. We highly recommend you keep the default settings.

Status Information
The Broadband router's status information provides the following information about your Broadband router: Hardware/Firmware version, Serial Number, and its current operating status.

Tools
Broadband router Tools - Tools include Configuration tools, Firmware upgrade and Reset. Configuration tools allow you to Backup, Restore, or Restore to Factory Default setting for your Broadband router. The Firmware upgrade tool allows you to upgrade your Broadband router's firmware. The RESET tool allows you to reset your Broadband router.

The left panel provides four options, **Quick Setup**, **General Setup**, **Status Information** and **Tools**.

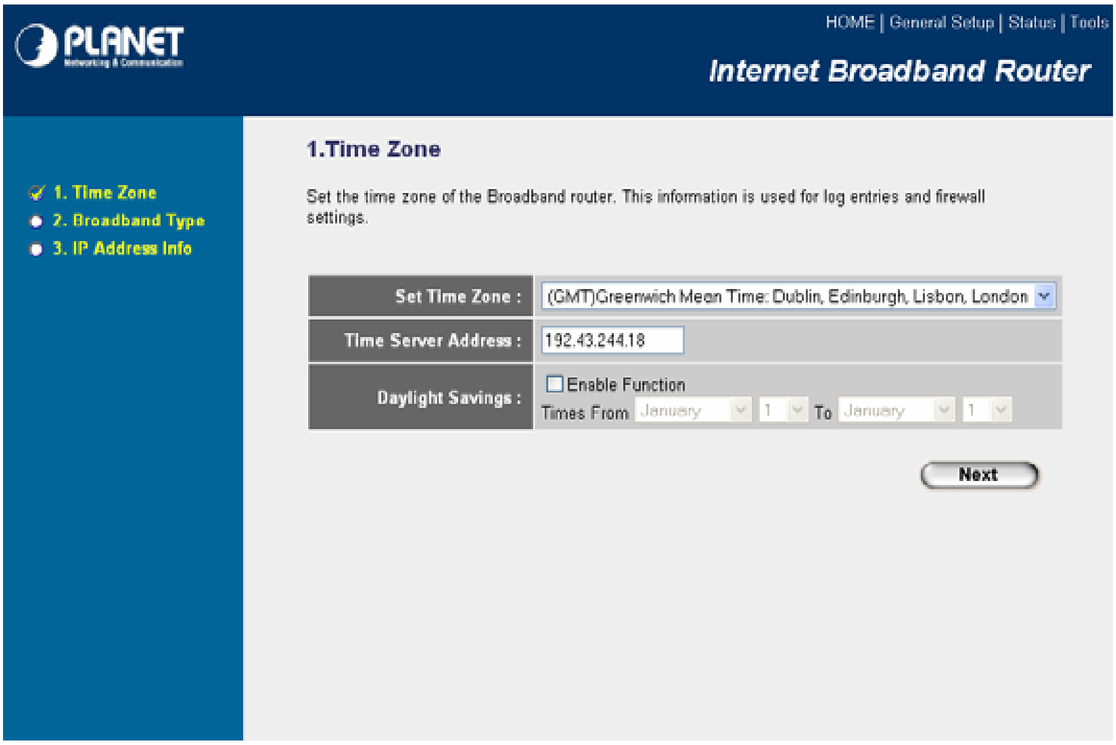
Section	Description
Quick Setup	Select your Internet connection type and then input the configurations needed to connect to your Internet Service Provider (ISP).
General Setup	This section contains configurations for the Broadband router’s advance functions such as: Port Forwarding, Virtual Server, Access Control, Hacker Attack Prevention, DMZ, Special applications and other functions to meet your LAN requirements. You can also configure the wireless detail settings here.
Status Info	This option provides you the system information, Internet Connection, Device Status, Security Log and DHCP client Log information.
Tools	This option contains Configuration tools, Firmware Upgrade and Reset functions.

Chapter 4 Quick Setup

This section describes the basic configuration of the WMRT-414 and allows you to connect to Internet easily.

4.1 Time Zone

The time information is used for Log entries and Firewall settings. You can keep the default Time Server address or set a new IP address for your router to synchronize its time. Click “Next” to continue.


PLANET
Networking & Communication
HOME | General Setup | Status | Tools
Internet Broadband Router
1. Time Zone
2. Broadband Type
3. IP Address Info
Next

1.Time Zone

Set the time zone of the Broadband router. This information is used for log entries and firewall settings.

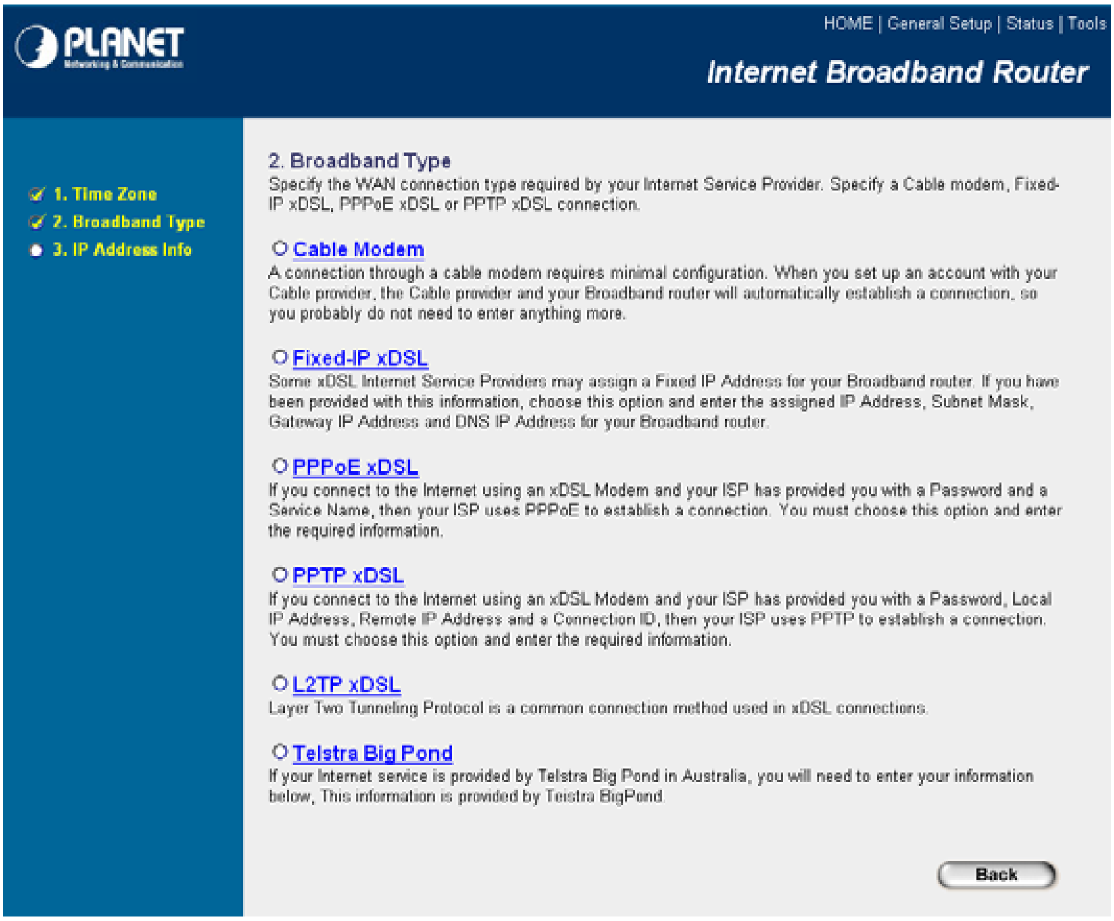
Set Time Zone :	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
Time Server Address :	192.43.244.18
Daylight Savings :	□ Enable Function Times From January 1 To January 1

Parameter	Description
Set Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.
Time Server Address	Remain it as default or, you can manually assign an IP address of the Time Server. The information of Timer Server can be found in the following URL link: http://www.eecis.udel.edu/~mills/ntp/servers.html or http://www.ntp.org.
Enable Daylight Savings	The router can also take Daylight savings into account. To enable this function, check/tick the “Enable Function” box and select which days this function will work.

Click “Next” button to proceed to the next step.

4.2 Broadband Type

Before establishing the Internet connection, please be sure to check with your ISP, and obtain all necessary information from them.


PLANET
Networking & Communication
HOME | General Setup | Status | Tools
Internet Broadband Router
1. Time Zone
2. Broadband Type
3. IP Address Info
Back

2. Broadband Type

Specify the WAN connection type required by your Internet Service Provider. Specify a Cable modem, Fixed-IP xDSL, PPPoE xDSL or PPTP xDSL connection.

○ Cable Modem

A connection through a cable modem requires minimal configuration. When you set up an account with your Cable provider, the Cable provider and your Broadband router will automatically establish a connection, so you probably do not need to enter anything more.

○ Fixed-IP xDSL

Some xDSL Internet Service Providers may assign a Fixed IP Address for your Broadband router. If you have been provided with this information, choose this option and enter the assigned IP Address, Subnet Mask, Gateway IP Address and DNS IP Address for your Broadband router.

○ PPPoE xDSL

If you connect to the Internet using an xDSL Modem and your ISP has provided you with a Password and a Service Name, then your ISP uses PPPoE to establish a connection. You must choose this option and enter the required information.

○ PPTP xDSL

If you connect to the Internet using an xDSL Modem and your ISP has provided you with a Password, Local IP Address, Remote IP Address and a Connection ID, then your ISP uses PPTP to establish a connection. You must choose this option and enter the required information.

○ L2TP xDSL

Layer Two Tunneling Protocol is a common connection method used in xDSL connections.

○ Telstra Big Pond

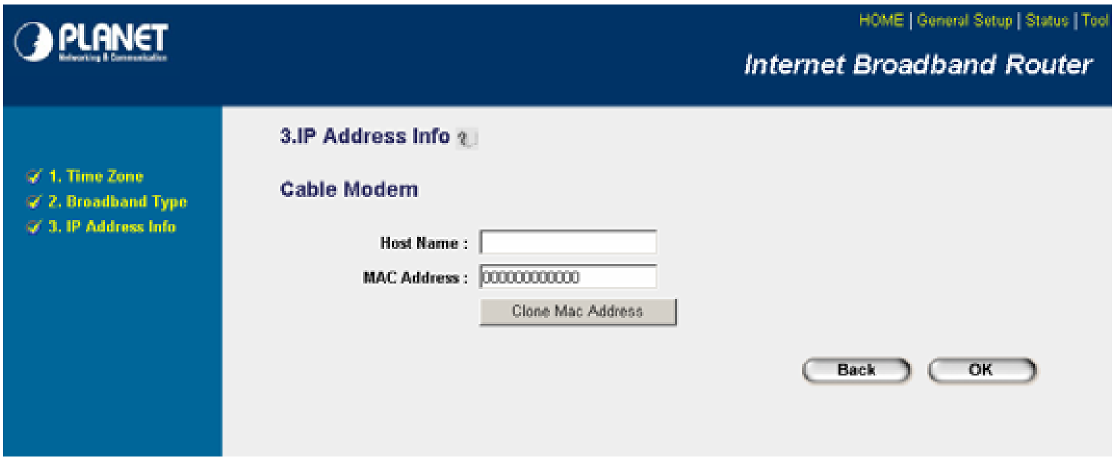
If your Internet service is provided by Telstra Big Pond in Australia, you will need to enter your information below, This information is provided by Telstra BigPond.

Broadband	Description
Cable Modem	ISP will automatically give you an IP address. Please refer to section 4.2.1 for details.
Fixed-IP xDSL	ISP has given you a fixed IP address already. Please refer to section 4.2.2 for details.
PPPoE xDSL	ISP requires you to use a Point-to-Point Protocol over Ethernet (PPPoE) connection. Please refer to section 4.2.3 for details.
PPTP xDSL	ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection. Please refer to section 4.2.4 for details.
L2TP XDSL	This is not widely used. You need to know the PPTP Server address as well as your name and password. Please refer to section 4.2.5 for details.
Telstra Big Pond	This option is for Australia only. Please refer to section 4.2.6 for details.

4.2.1 Cable Modem

With Cable Modem connection, the ISP will automatically give you an IP address. Some ISP may also require you to fill in additional information such as Host Name and MAC address (see screen below).

Note: The Host Name and MAC address section is **optional** and you can skip this section if your ISP does not require these settings for you to connect to the Internet.



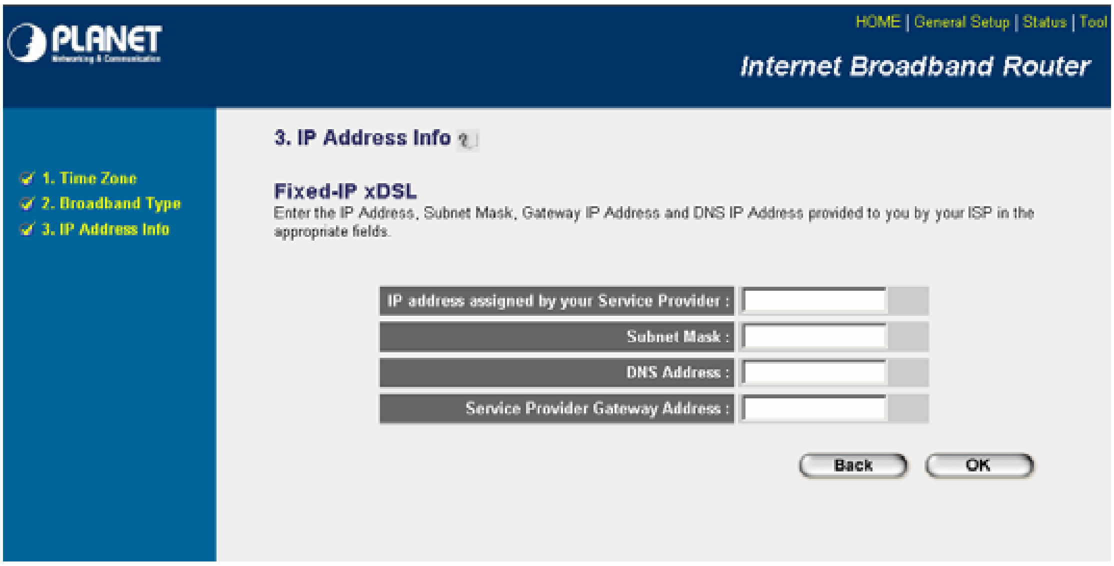
Host Name :
MAC Address : 000000000000

Parameters	Description
Host Name	Type in the host name provided by your ISP if any; otherwise, just leave it blank.
MAC Address	To connect to Internet, your ISP will require a MAC address from your PC. Type in this MAC address in this section or use the "**Clone MAC Address**" button to replace the WAN port MAC address with the your PC's. To find out the PC's MAC address, see Appendix A. (also see Glossary for an explanation on MAC address).

When the configuration finished, click "OK" to next step or click "Back" to previous step. After press "OK", you will see a web screen to prompt you the configurations save successfully. Please refer to section 4.2.7 for the information of this screen.

4.2.2 Fixed-IP xDSL

Select Fixed-IP xDSL if your ISP has given you a specified IP address. Your ISP should provide all the information required in this section.



PLANET
HOME | General Setup | Status | Tool
Internet Broadband Router
1. Time Zone
2. Broadband Type
3. IP Address Info
Back
OK

3. IP Address Info

Fixed-IP xDSL

Enter the IP Address, Subnet Mask, Gateway IP Address and DNS IP Address provided to you by your ISP in the appropriate fields.

IP address assigned by your Service Provider :

Subnet Mask :

DNS Address :

Service Provider Gateway Address :

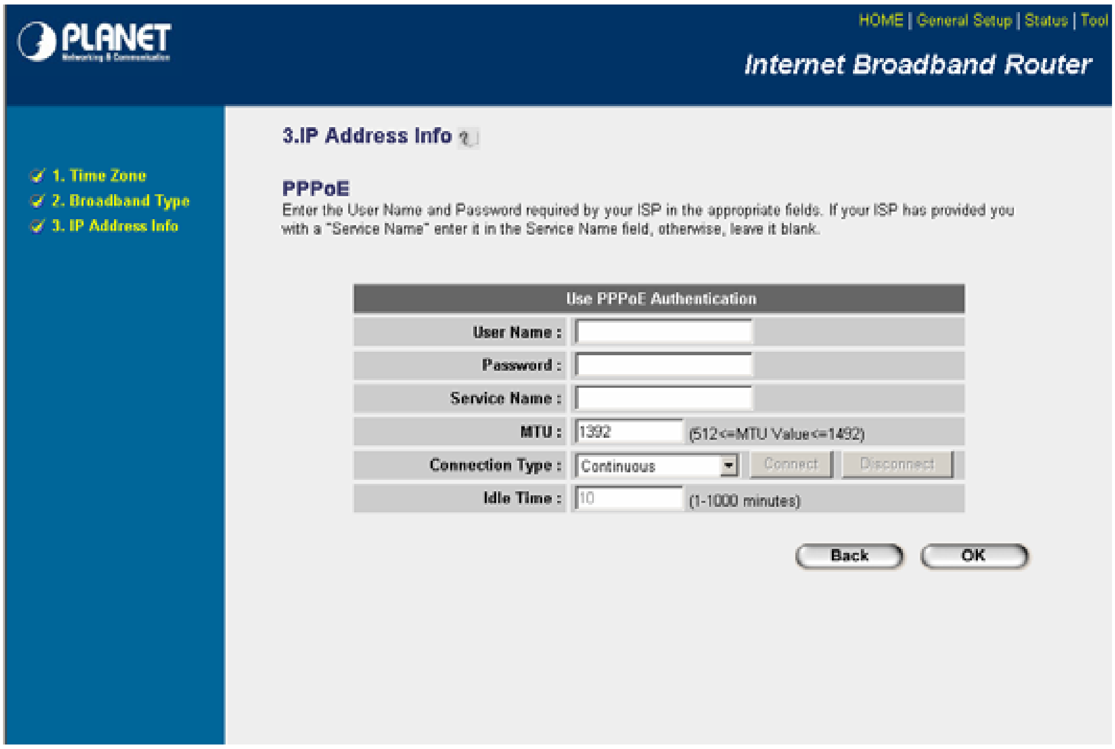
Parameters	Description
IP address assigned by your Service Provider	The IP address that your ISP should provide you.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0).
DNS Address	The IP address of ISP's DNS (Domain Name Service) Server.
Service Provider Gateway Address	The ISP's IP address gateway.

Please consult your local ISP about the information above.

When the configuration finished please click “OK” to next step or click “Back” to previous step. After press “OK”, you will see a web screen to prompt you the configurations save successfully. Please refer to section 4.2.7 for the information of this screen.

4.2.3 PPPoE xDSL

Select PPPoE if your ISP requires the PPPoE protocol for Internet connectivity. Your ISP should provide all the information like user name, password required in this section.


HOME | General Setup | Status | Tool
Internet Broadband Router
1. Time Zone
2. Broadband Type
3. IP Address Info

3.IP Address Info

PPPoE

Enter the User Name and Password required by your ISP in the appropriate fields. If your ISP has provided you with a "Service Name" enter it in the Service Name field, otherwise, leave it blank.

Use PPPoE Authentication	
User Name :	
Password :	
Service Name :	
MTU :	1392 (512<=MTU Value<=1492)
Connection Type :	Continuous ▾ Connect Disconnect
Idle Time :	10 (1-1000 minutes)

Back OK

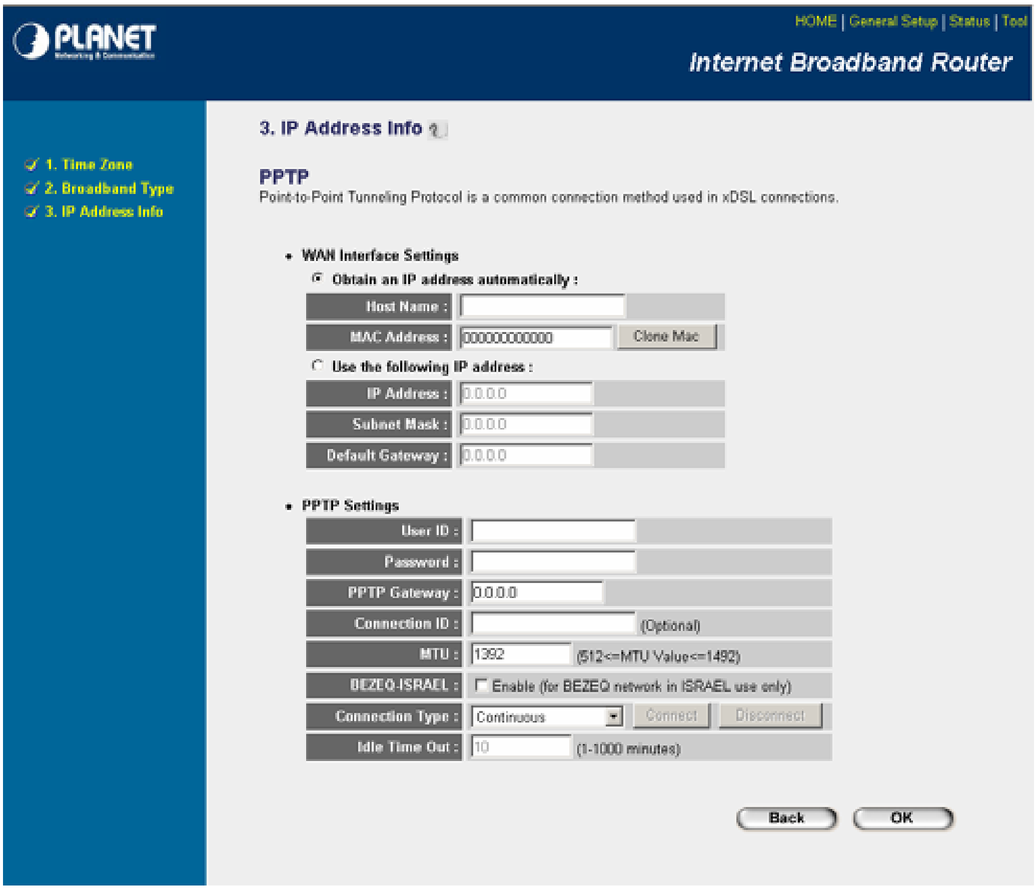
Parameters	Description
User Name	Enter the User Name provided by your ISP for the PPPoE connection.
Password	Enter the Password provided by your ISP for the PPPoE connection.
Service Name	This is an optional parameter. Leave it blank unless your ISP requires it.
MTU	This is an optional parameter. You can specify the maximum size of transmission packet to the Internet. The range of the MTU will be from 512 to 1492. You can also consult you ISP for the optimal MTU as well. Default: 1392.
Connection Type	If you select "**Continuous**", the router will always connect to the ISP. If the WAN line breaks down and links again, the router will auto-reconnect to the ISP. If you select "**Connect On Demand**", the router will auto-connect to the ISP when a client in LAN want to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "**Idle Time**". If you select "**Manual**", the router will connect to ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not disconnect due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP. Default: **Continuous**.
Idle Time	You can specify an idle time threshold (minutes) for the WAN port. This means if no

	packets have been sent (no one using the Internet) during this specified period, the router will automatically disconnect the connection from your ISP. **Note:** This “idle timeout” function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly, especially when your ISP charges you by time used.

When the configuration finished, click “OK” to next step or click “Back” to previous step. After press “OK”, you will see a web screen to prompt you the configurations save successfully. Please refer to section 4.2.7 for the information of this screen.

4.2.4 PPTP xDSL

Select PPTP if your ISP requires the PPTP protocol to connect to the Internet. Your ISP should provide all the information required in this section.



3. IP Address Info

PPTP

Point-to-Point Tunneling Protocol is a common connection method used in xDSL connections.

- WAN Interface Settings

● Obtain an IP address automatically :

Host Name :	
MAC Address :	000000000000 Clone Mac

○ Use the following IP address :

IP Address :	0.0.0.0
Subnet Mask :	0.0.0.0
Default Gateway :	0.0.0.0

- PPTP Settings

User ID :	
Password :	
PPTP Gateway :	0.0.0.0
Connection ID :	(Optional)
MTU :	1392 (512<=MTU Value<=1492)
BEZEQ-ISRAEL :	□ Enable (for BEZEQ network in ISRAEL use only)
Connection Type :	Continuous ▾ Connect Disconnect
Idle Time Out :	10 (1-1000 minutes)

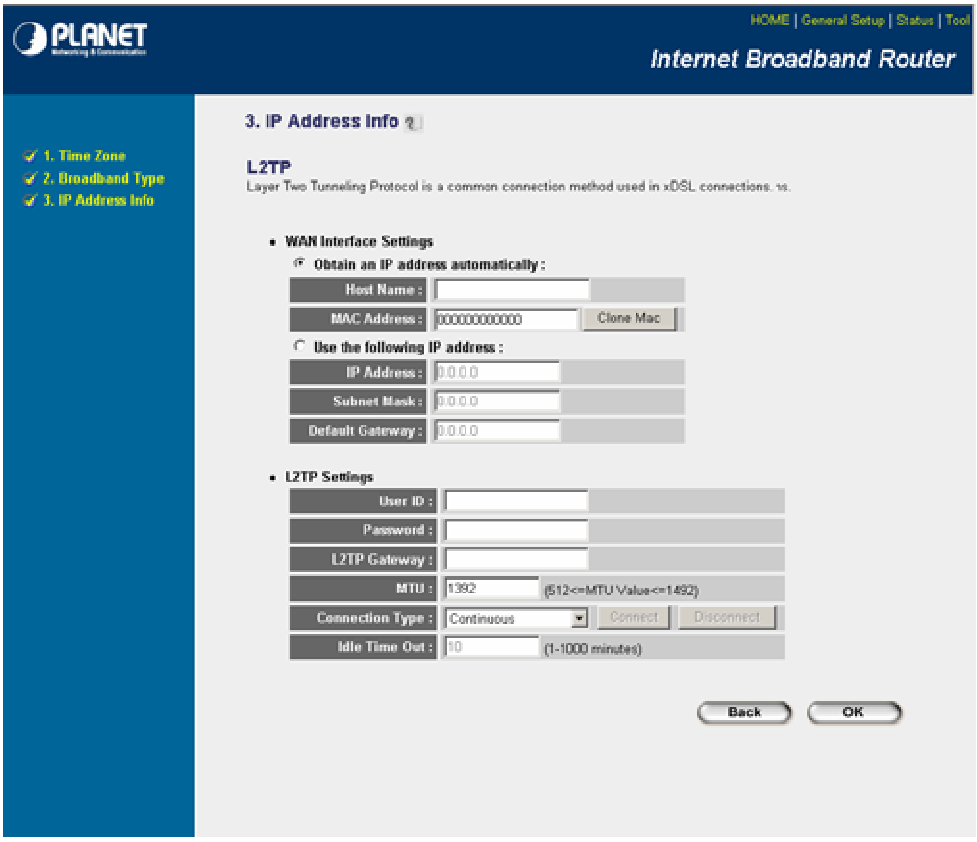
Parameter	Description
Obtain an IP address	Select it if the ISP requires you to obtain an IP address by DHCP automatically.
Host Name	Type in the host name provided by your ISP if any; otherwise, just leave it blank.
MAC Address	To connect to the Internet, your ISP will require a MAC address from your PC. Type in this MAC address in this section or use the "Clone MAC Address" button to replace the WAN port MAC address with the MAC address of that PC. To find out the PC's MAC address, see Appendix A. (also see Glossary for an explanation on MAC address).
Use the following IP address	Select it if the ISP provides you a static IP to connect to the PPTP server.
IP Address	This is the IP address that your ISP has given you to establish a PPTP connection.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0)
Gateway	Enter the IP address of the ISP's Gateway.
User ID	Enter the User Name provided by your ISP for the PPTP connection. Sometimes called a Connection ID.
Password	Enter the Password provided by your ISP for the PPTP connection
PPTP Gateway	If your LAN has a PPTP gateway, enter that PPTP gateway's IP address here. If you do not have a PPTP gateway, enter the ISP's Gateway IP address above.
Connection ID	This is the ID given by ISP. This is an optional parameter.
MTU	This is an optional parameter. You can specify the maximum size of transmission packet to the Internet. The range of the MTU will be from 512 to 1492. You can also consult you ISP for the optimal MTU as well. Default: 1392
BEZEQ-ISRAEL	Select this item if you are using the service provided by BEZEQ in Israel.
Connection Type	If you select "**Continuous**", the router will always connect to the ISP. If the WAN line breaks down and links again, the router shall auto- reconnect to the ISP. If you select "**Connect On Demand**", the router will auto-connect to the ISP when a client in LAN wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "Idle Time". If you select "**Manual**", the router will connect to ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not disconnected due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP. Default: **Continuous.**
Idle Time	You can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent (no one using the Internet) throughout this specified period, the router will automatically disconnect to with your ISP. **Note:** This "idle timeout" function may not work due to abnormal activities of

	some network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly, especially when your ISP charges you by time used.

When the configuration finished please click “OK” to next step or click “Back” to previous step. After press “OK”, you will see a web screen to prompt you the configurations save successfully. Please refer to section 4.2.7 for the information of this screen.

4.2.5 L2TP xDSL

Select L2TP if your ISP requires the L2TP protocol to connect to the Internet. Your ISP should provide all the information required in this section.



3. IP Address Info

L2TP

Layer Two Tunneling Protocol is a common connection method used in xDSL connections. 1s.

- WAN Interface Settings
  - ● Obtain an IP address automatically :
    - Host Name :
    - MAC Address : 000000000000
  - ○ Use the following IP address :
    - IP Address : 0.0.0.0
    - Subnet Mask : 0.0.0.0
    - Default Gateway : 0.0.0.0
- L2TP Settings
  - User ID :
  - Password :
  - L2TP Gateway :
  - MTU : 1392 (512<=MTU Value<=1492)
  - Connection Type : Continuous
  - Idle Time Out : 10 (1-1000 minutes)

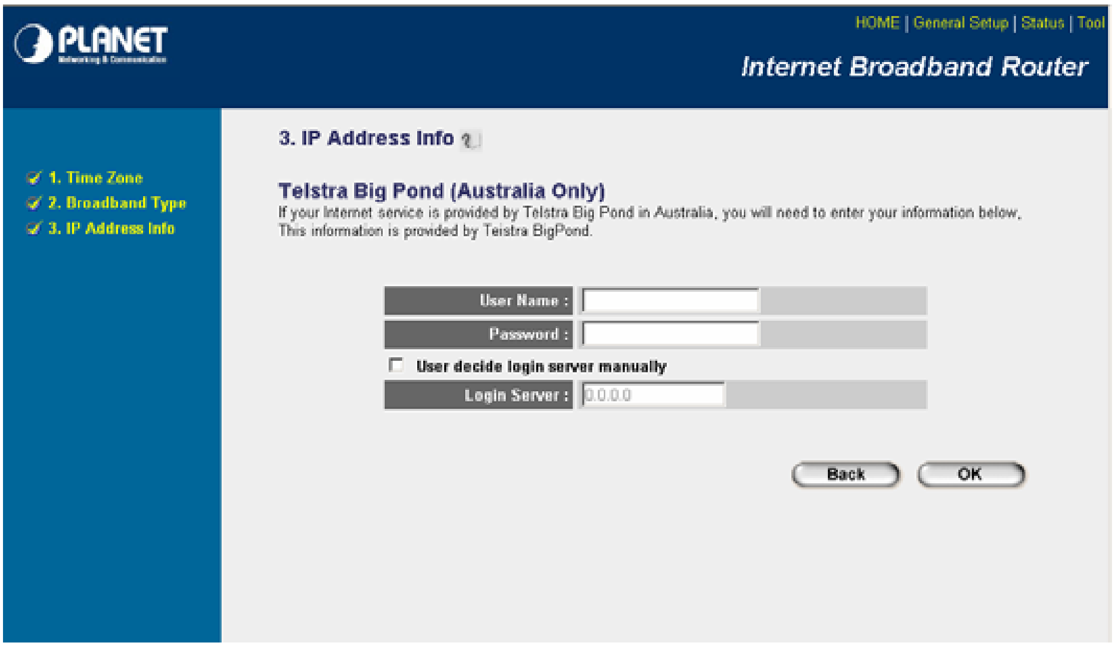
Parameter	**Description**
Obtain an IP address	Select it if the ISP requires you to obtain an IP address by DHCP automatically.
Host Name	If your ISP requires a Host Name, type in the host name provided by your ISP; otherwise, just leave it blank.
MAC Address	To connect to the Internet, your ISP will require a MAC address from your PC. Type in this MAC address in this section or use the “Clone MAC Address”

	button to replace the WAN port MAC address with the MAC address of that PC. To find out the PC's MAC address, see Appendix A. (also see Glossary for an explanation on MAC address.
Use the following IP address	Select it if the ISP provides you a static IP to connect to the L2TP server.
IP Address	This is the IP address that your ISP has given you to establish a L2TP connection.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0)
Gateway	Enter the IP address of the ISP's Gateway.
User ID	Enter the User Name provided by your ISP for the L2TP connection. Sometimes called a Connection ID.
Password	Enter the Password provided by your ISP for the L2TP connection
L2TP Gateway	If your LAN has a L2TP gateway, enter that L2TP gateway's IP address here. If you do not have a L2TP gateway, enter the ISP's Gateway IP address above.
MTU	This is an optional parameter. You can specify the maximum size of transmission packet to the Internet. The range of the MTU will be from 1492 to 512. You can also consult you ISP for the optimal MTU as well. Default: 1392
Connection Type	If you select "**Continuous**", the router will always connect to the ISP. If the WAN line breaks down and links again, the router shall auto- reconnect to the ISP. If you select "**Connect On Demand**", the router will auto-connect to the ISP when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "Idle Time". If you select "**Manual**", the router will connect to ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not disconnect due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP. Default: **Continuous.**
Idle Time	You can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent (no one using the Internet) throughout this specified period, then the router will automatically disconnect the connection with your ISP. **Note:** This "idle timeout" function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly, especially when your ISP charges you by time used.

When the configuration finished please click “OK” to next step or click “Back” to previous step. After press “OK”, you will see a web screen to prompt you the configurations save successfully. Please refer to section 4.2.7 for the information of this screen.

4.2.6 Telstra Big Pond

Select Telstra Big Pond if you are live in Australia and your ISP requires this protocol to connect to the Internet. Your ISP should provide all the information required in this section.



PLANET
HOME | General Setup | Status | Tool
Internet Broadband Router
1. Time Zone
2. Broadband Type
3. IP Address Info
Back
OK

3. IP Address Info

Telstra Big Pond (Australia Only)

If your Internet service is provided by Telstra Big Pond in Australia, you will need to enter your information below. This information is provided by Telstra BigPond.

User Name :

Password :

□ User decide login server manually

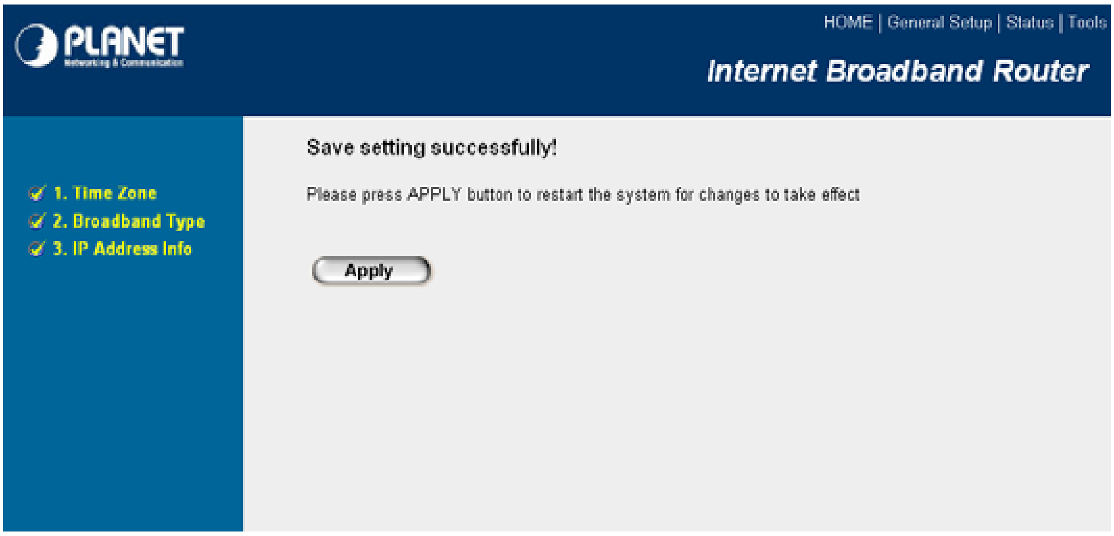
Login Server : 0.0.0.0

Parameters	Description
User Name	Enter the User Name provided by your ISP for the connection.
Password	Enter the Password provided by your ISP for the connection.
User Decide login server manually	If you ISP has provide the login server IP address to you, please check this box and enter the Login Server IP address below.
Login Server	Please enter the Login Server IP address here.

When the configuration finished please click “OK” to next step or click “Back” to previous step. After press “OK”, you will see a web screen to prompt you the configurations save successfully. Please refer to section 4.2.7 for the information of this screen.

4.2.7 Save Settings Successfully

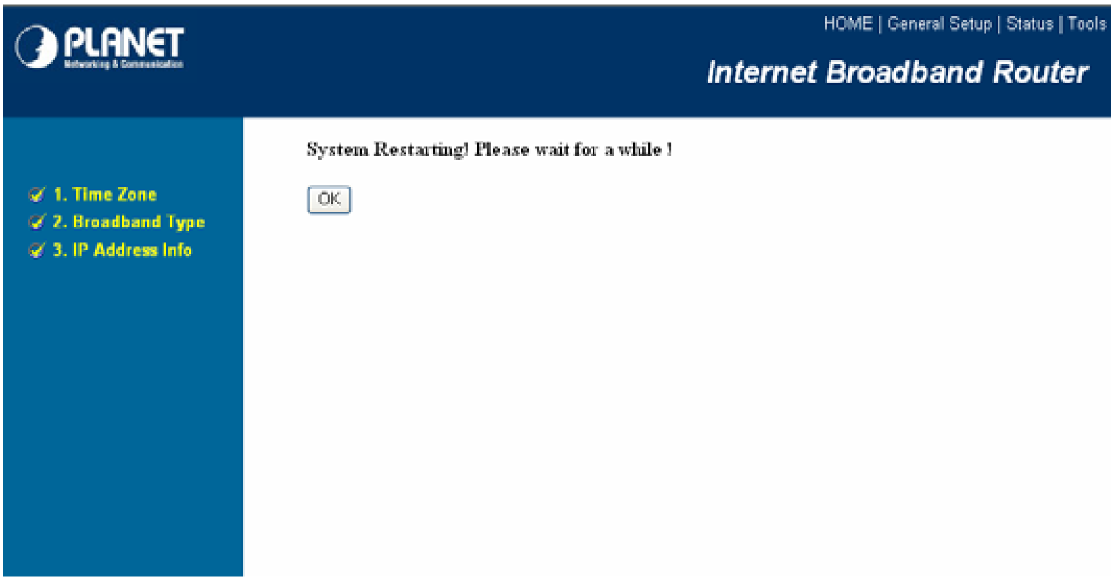
When you press “OK” in above configuration, the settings will be saved and the screen appears as below. Before WMRT-414 restart, the settings are saved, but not function yet. Press “Apply” to restart the WMRT-414 for the change to take effect immediately.


PLANET
Networking & Communication
HOME | General Setup | Status | Tools
Internet Broadband Router
1. Time Zone
2. Broadband Type
3. IP Address Info

Save setting successfully!

Please press APPLY button to restart the system for changes to take effect

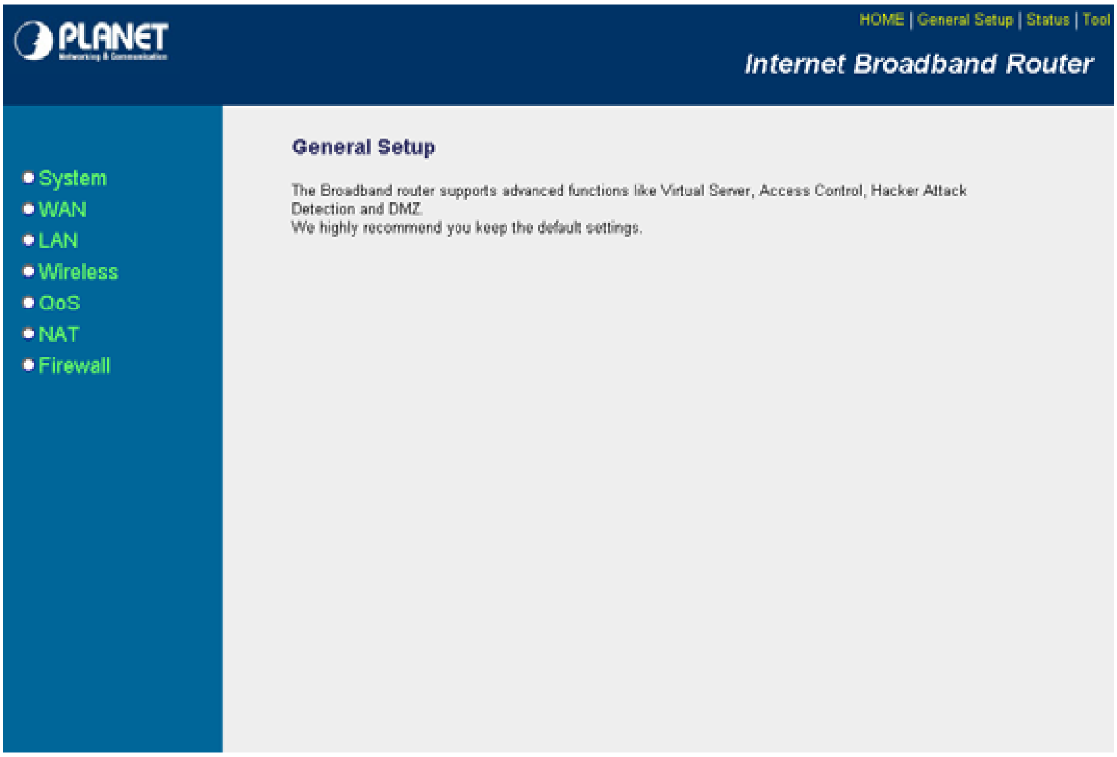
Please wait for 30 seconds for WMRT-414 restart. After restart procedure finished, please click “OK” to return to HOME screen.


PLANET
Networking & Communication
HOME | General Setup | Status | Tools
Internet Broadband Router
1. Time Zone
2. Broadband Type
3. IP Address Info

System Restarting! Please wait for a while !

Chapter 5 General Setup

After click on the “General Setup” button at the main Page, you should see the screen below.



PLANET
Networking & Communication
HOME | General Setup | Status | Tool
Internet Broadband Router
System
WAN
LAN
Wireless
QoS
NAT
Firewall

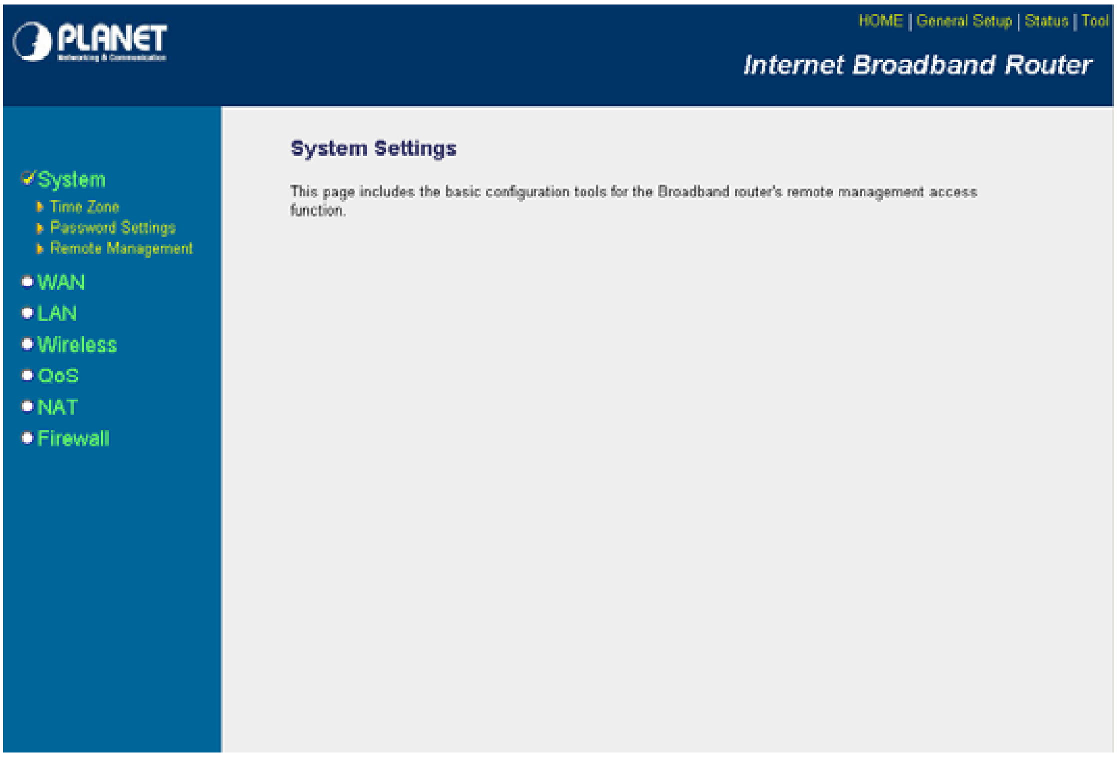
General Setup

The Broadband router supports advanced functions like Virtual Server, Access Control, Hacker Attack Detection and DMZ.
We highly recommend you keep the default settings.

The General Setup contains advanced features that allow you to configure the router to meet the network’s needs such as: Wireless, Port Forwarding, Virtual Server, Access Control, URL Blocking, Special Applications, DMZ and other functions.

5.1 System

This section shows how to setup the Broadband router’s system Time Zone, Password and Remote Management Administrator.



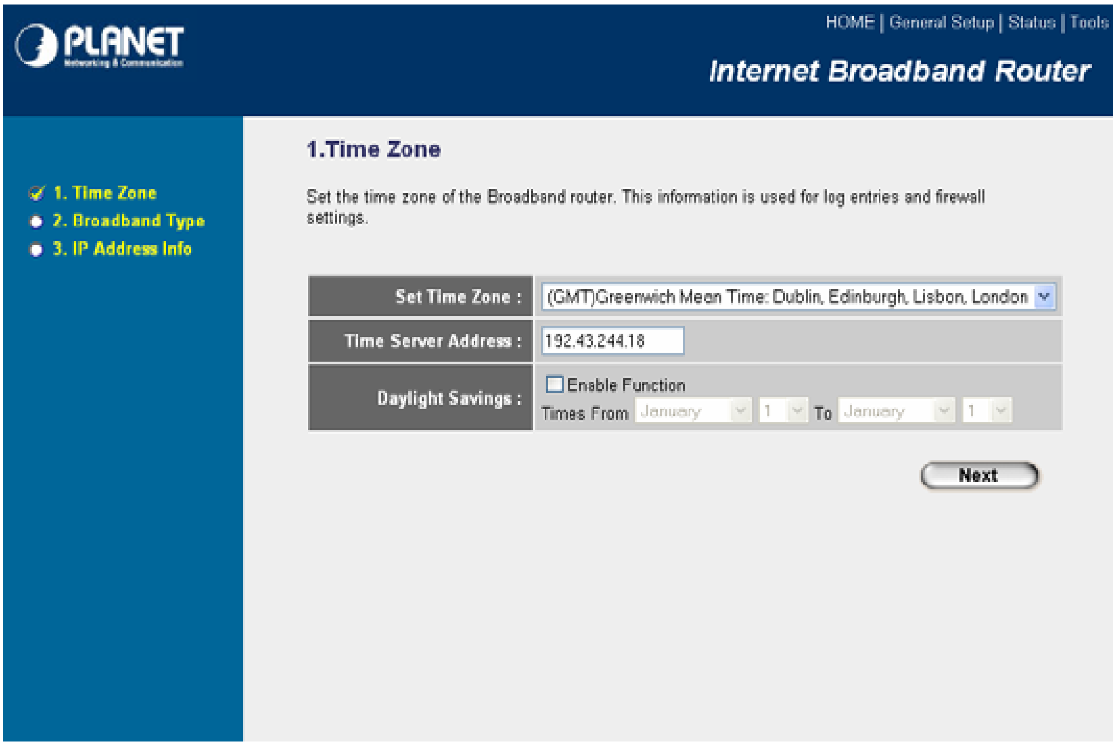
PLANET
Networking & Communication
HOME | General Setup | Status | Tool
Internet Broadband Router
System
Time Zone
Password Settings
Remote Management
WAN
LAN
Wireless
QoS
NAT
Firewall

System Settings

This page includes the basic configuration tools for the Broadband router's remote management access function.

5.1.1 Time Zone

The Time Zone allows WMRT-414 to allocate its time with the settings configured; it will affect log display functions such as Security Log and Firewall settings.


HOME | General Setup | Status | Tools
Internet Broadband Router
✓ 1. Time Zone
● 2. Broadband Type
● 3. IP Address Info
Next

1.Time Zone

Set the time zone of the Broadband router. This information is used for log entries and firewall settings.

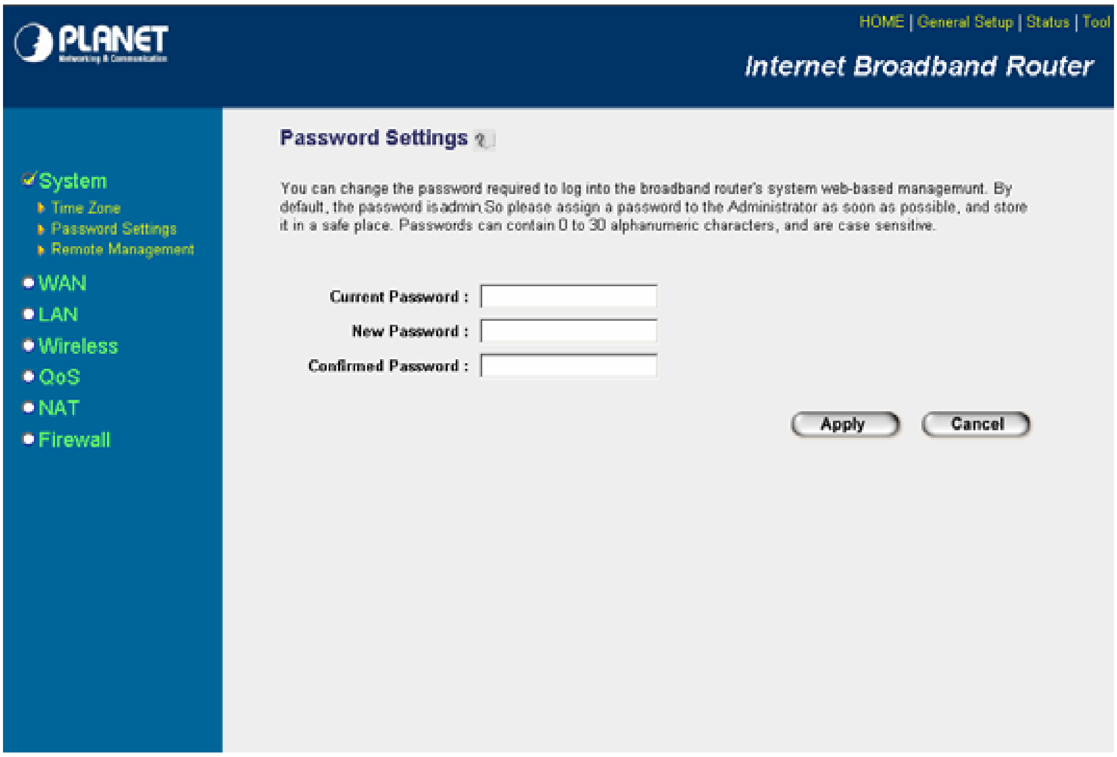
Set Time Zone :	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
Time Server Address :	192.43.244.18
Daylight Savings :	□ Enable Function Times From January 1 To January 1

Parameter	Description
Set Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.
Time Server Address	You can keep the default IP address or enter a new Time Server Address for this device to synchronize its time. You can also refer to the web site http://www.ntp.org to find a nearest time server.
Daylight Savings	The router can also take Daylight savings into account. Select the check box to enable your daylight saving configuration. You can set the days that you wish to start and stop daylight Savings Time.

After the setup completed, please click “Apply” to save the settings. After press “Apply”, you will see a web screen to prompt you the configurations save successfully. You may refer to section 4.2.7 for the information of this screen.

5.1.2 Password Setup

This screen allows you to change the management password.



Password Settings

You can change the password required to log into the broadband router's system web-based managemunt. By default, the password is admin So please assign a password to the Administrator as soon as possible, and store it in a safe place. Passwords can contain 0 to 30 alphanumeric characters, and are case sensitive.

Current Password :

New Password :

Confirmed Password :

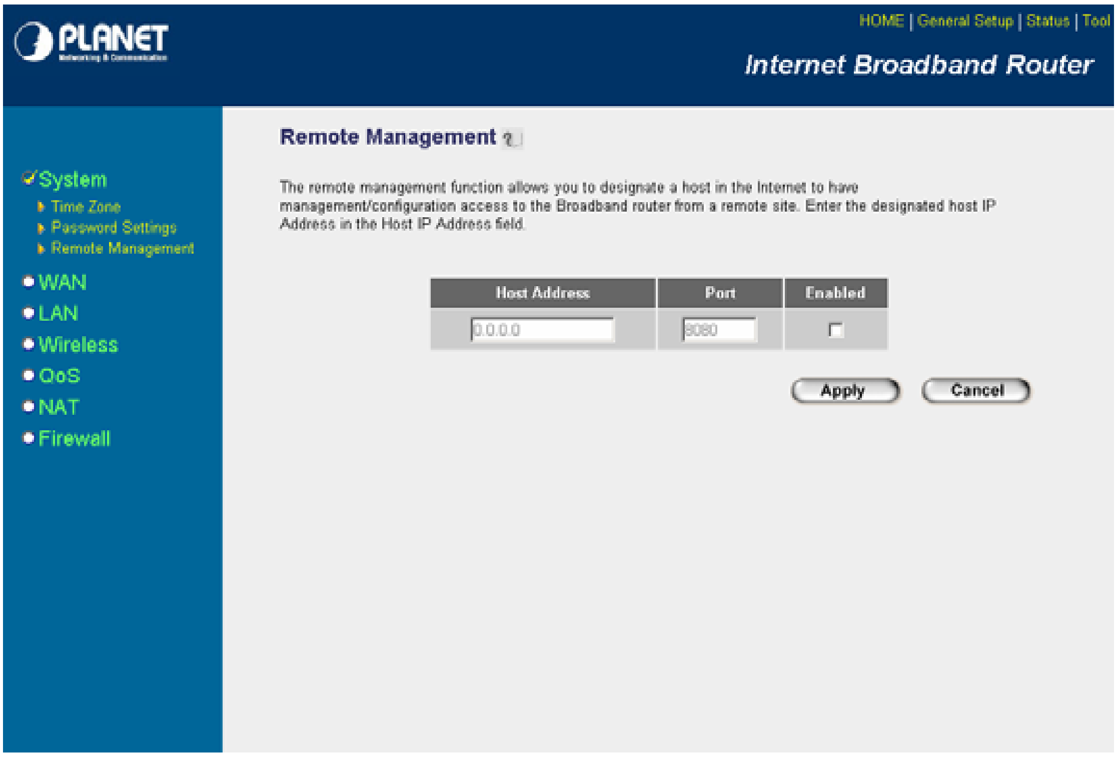
Parameters	Description
Current Password	Enter your current password for the remote management administrator to login to your Broadband router.
New Password	Enter your new password.
Confirmed Password	Enter your new password again for verification purposes.

After the setup completed, please click “Apply” to save the settings. After press “Apply”, you will see a web screen to prompt you the configurations save successfully. You may refer to section 4.2.7 for the information of this screen.

Note: If you forget the password, please reset the WMRT-414 to the factory default by press **RESET** button (on WMRT-414’s rear panel) over 10 seconds.

5.1.3 Remote Management

You can specify a Host IP address that can perform remote management from Internet.



Remote Management

The remote management function allows you to designate a host in the Internet to have management/configuration access to the Broadband router from a remote site. Enter the designated host IP Address in the Host IP Address field.

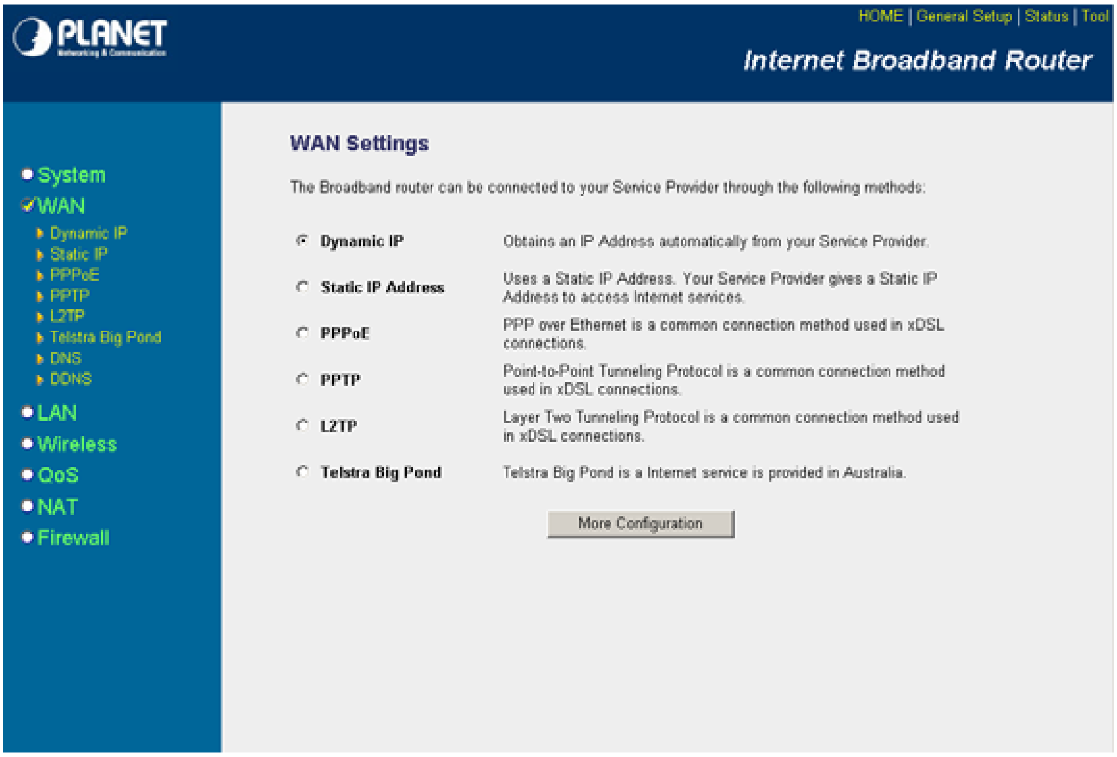
Host Address	Port	Enabled
0.0.0.0	8080	□

Parameters	Description
Host Address	The IP address of the host on Internet that will have management / configuration access to the Broadband router. Leave it to **0.0.0.0** means anyone can access the router’s web-based configuration from any remote location. Click the **Enabled** box to enable the Remote Management function. **Note:** When you want to access the web-based management from a remote site, you must enter the router’s WAN IP address (e.g. 10.0.0.1) into your web-browser followed by port number 8080, e.g. 10.0.0.1:8080 (see below). You’ll also need to know the password set in the Password Setting screen in order to access the management pages.

After the setup completed, please click “Apply” to save the settings. After press “Apply”, you will see a web screen to prompt you the configurations save successfully. You may refer to section 4.2.7 for the information of this screen.

5.2 WAN

The WAN Settings screen allows you to specify the type of Internet connection. The WAN settings offer the following selections for the router's WAN port, **Dynamic IP**, **Static IP**, **PPPoE**, **PPTP**, **L2TP**, and **Telstra Big Pond**. Please select one of the connection types and click "More Configuration" button or select the option on the left window for configuration.



WAN Settings

The Broadband router can be connected to your Service Provider through the following methods:

● Dynamic IP — Obtains an IP Address automatically from your Service Provider.

○ Static IP Address — Uses a Static IP Address. Your Service Provider gives a Static IP Address to access Internet services.

○ PPPoE — PPP over Ethernet is a common connection method used in xDSL connections.

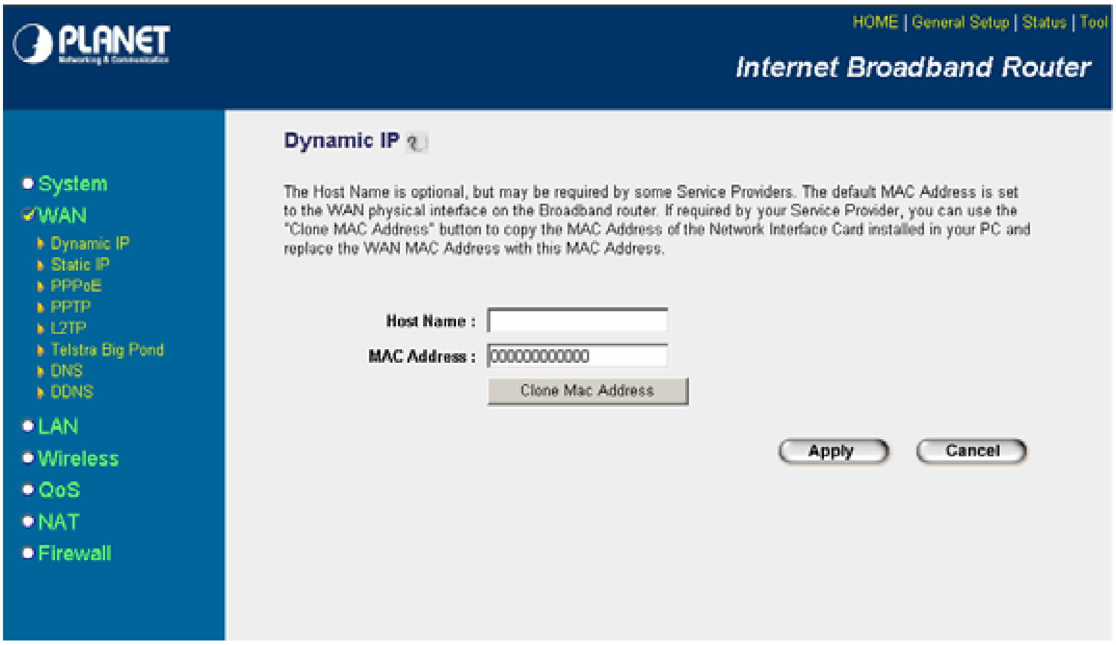
○ PPTP — Point-to-Point Tunneling Protocol is a common connection method used in xDSL connections.

○ L2TP — Layer Two Tunneling Protocol is a common connection method used in xDSL connections.

○ Telstra Big Pond — Telstra Big Pond is a Internet service is provided in Australia.

5.2.1 Dynamic IP

If Dynamic IP is selected, your ISP will automatically give you an IP address. Some ISP's may also require that you fill in additional information such as Host Name, Domain Name and MAC address. Please refer to the section 4.2.1 for more settings of this option.



Dynamic IP

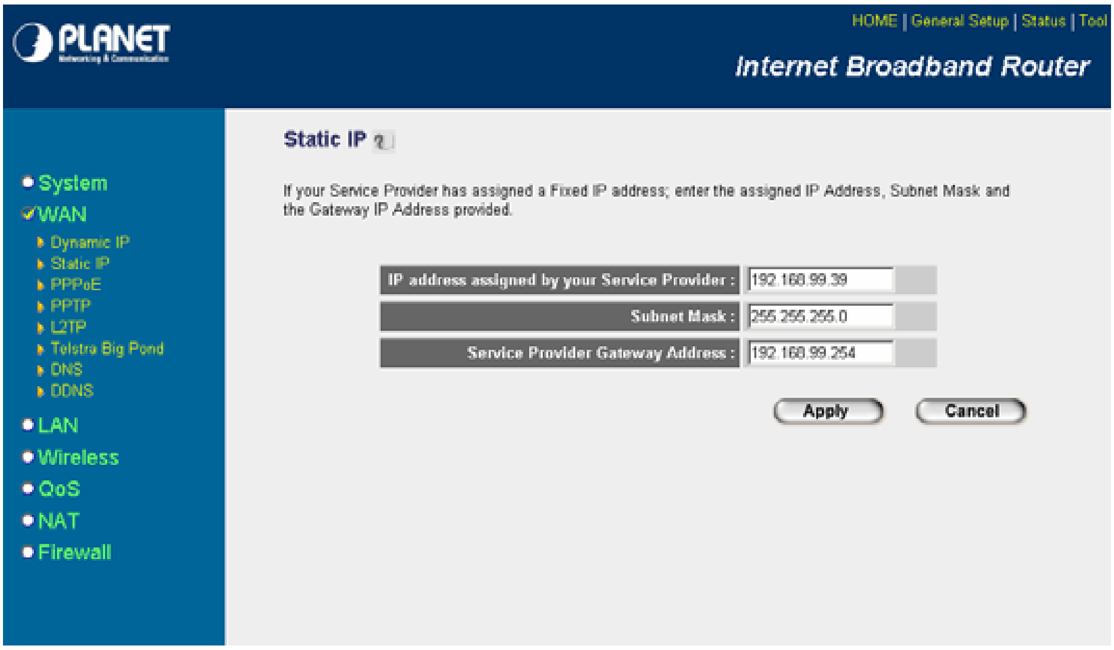
The Host Name is optional, but may be required by some Service Providers. The default MAC Address is set to the WAN physical interface on the Broadband router. If required by your Service Provider, you can use the "Clone MAC Address" button to copy the MAC Address of the Network Interface Card installed in your PC and replace the WAN MAC Address with this MAC Address.

Host Name :

MAC Address : 000000000000

5.2.2 Static IP

If Static IP is selected, your ISP should provide all the information required in this screen. Please refer to the section 4.2.2 for more settings of this option.



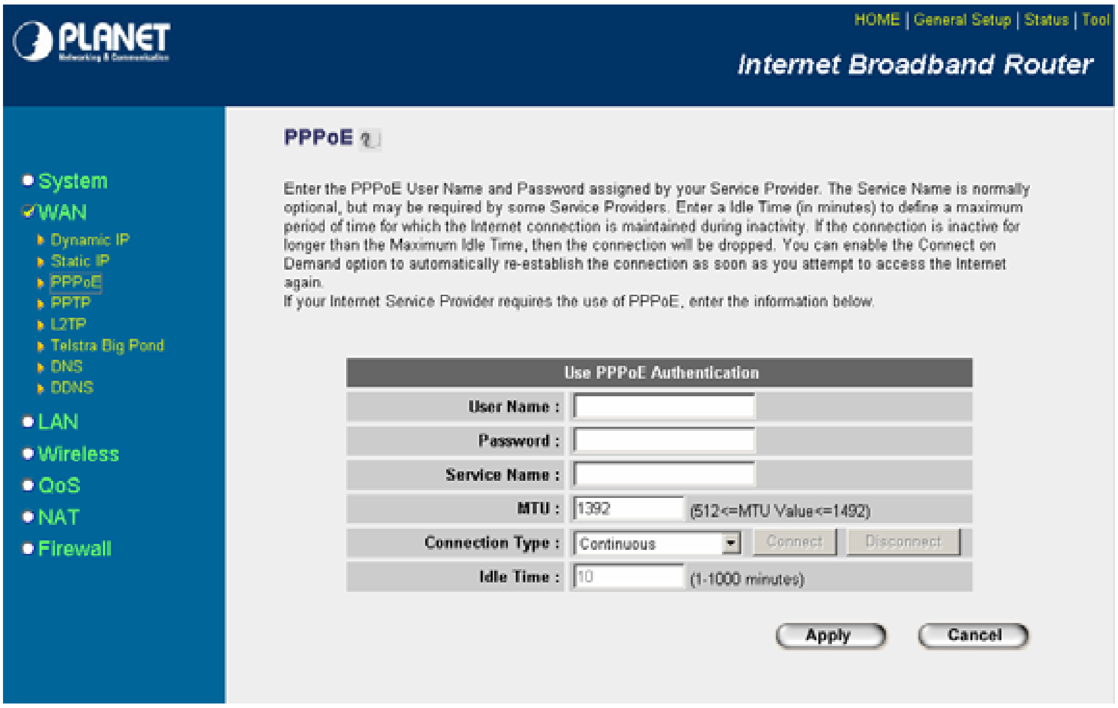
Static IP

If your Service Provider has assigned a Fixed IP address; enter the assigned IP Address, Subnet Mask and the Gateway IP Address provided.

IP address assigned by your Service Provider :	192.168.99.39
Subnet Mask :	255.255.255.0
Service Provider Gateway Address :	192.168.99.254

5.2.3 PPPoE

Select PPPoE if your ISP requires PPPoE protocol to connect to the Internet. Your ISP should provide all the information required in this section. Please refer to the section 4.2.3 to know the detail settings of this option.



PPPoE

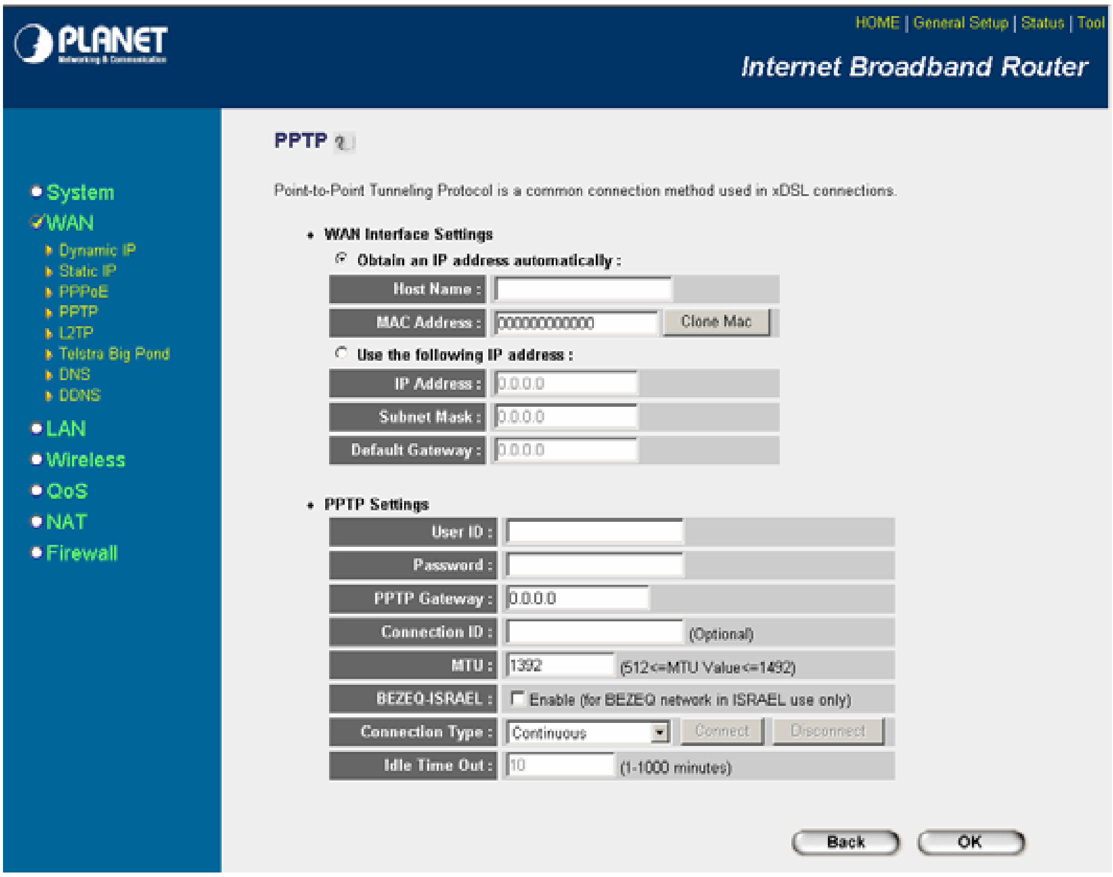
Enter the PPPoE User Name and Password assigned by your Service Provider. The Service Name is normally optional, but may be required by some Service Providers. Enter a Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then the connection will be dropped. You can enable the Connect on Demand option to automatically re-establish the connection as soon as you attempt to access the Internet again.

If your Internet Service Provider requires the use of PPPoE, enter the information below.

Use PPPoE Authentication	
User Name :	
Password :	
Service Name :	
MTU :	1392 (512<=MTU Value<=1492)
Connection Type :	Continuous
Idle Time :	10 (1-1000 minutes)

5.2.4 PPTP

Select PPTP if your ISP requires the PPTP protocol to connect to the Internet. Your ISP should provide all the information required in this section. Please refer to section 4.2.4 for more settings of this option.



PPTP

Point-to-Point Tunneling Protocol is a common connection method used in xDSL connections.

- WAN Interface Settings

● Obtain an IP address automatically :

Host Name :	
MAC Address :	000000000000

○ Use the following IP address :

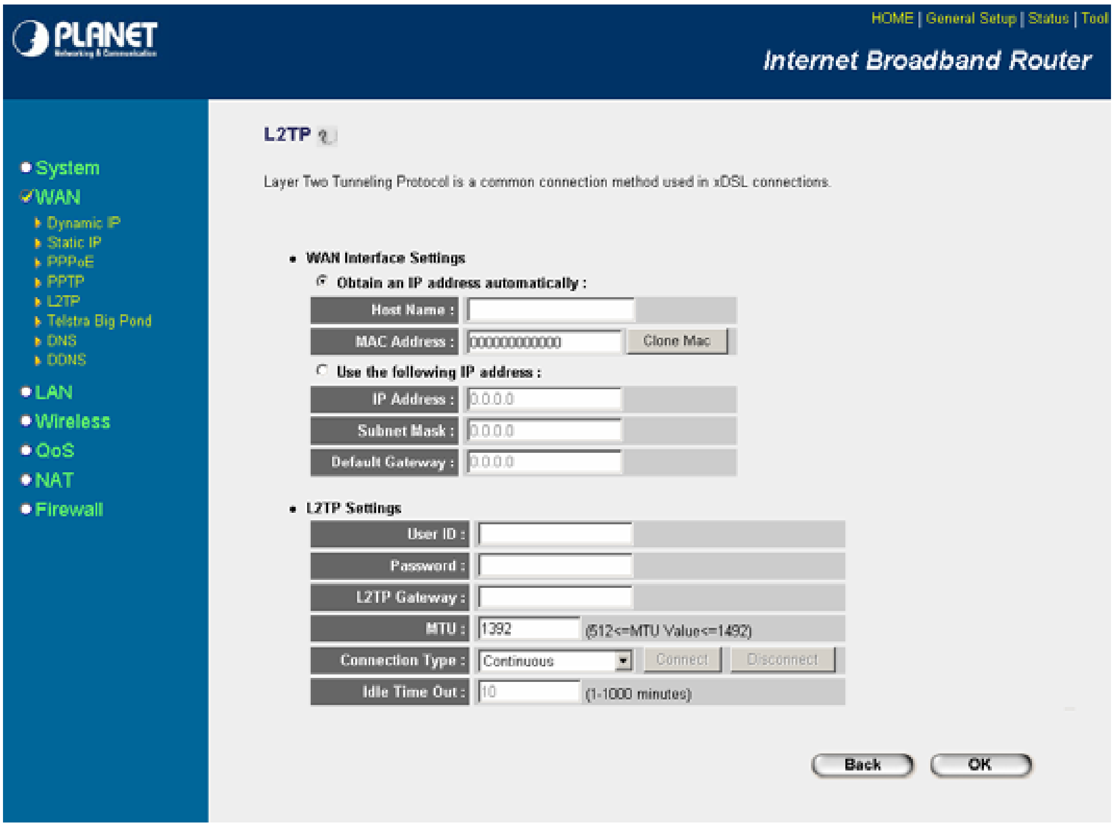
IP Address :	0.0.0.0
Subnet Mask :	0.0.0.0
Default Gateway :	0.0.0.0

- PPTP Settings

User ID :	
Password :	
PPTP Gateway :	0.0.0.0
Connection ID :	(Optional)
MTU :	1392 (512<=MTU Value<=1492)
BEZEQ-ISRAEL :	□ Enable (for BEZEQ network in ISRAEL use only)
Connection Type :	Continuous
Idle Time Out :	10 (1-1000 minutes)

5.2.5 L2TP

Select L2TP if your ISP requires the L2TP protocol to connect to the Internet. Your ISP should provide all the information required in this section. Please refer to section 4.2.5 for more settings of this option.



L2TP

Layer Two Tunneling Protocol is a common connection method used in xDSL connections.

- WAN Interface Settings

● Obtain an IP address automatically :

Host Name :	
MAC Address :	000000000000

○ Use the following IP address :

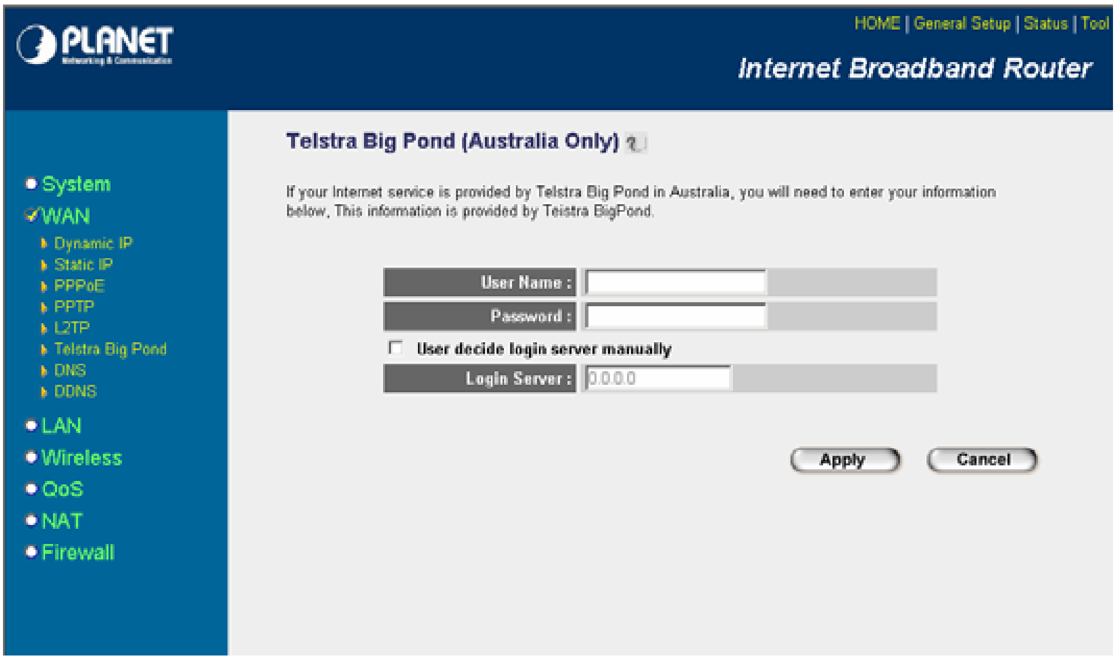
IP Address :	0.0.0.0
Subnet Mask :	0.0.0.0
Default Gateway :	0.0.0.0

- L2TP Settings

User ID :	
Password :	
L2TP Gateway :	
MTU :	1392 (512<=MTU Value<=1492)
Connection Type :	Continuous
Idle Time Out :	10 (1-1000 minutes)

5.2.6 Telstra Big Pond

Select Telstra Big Pond if your ISP is using this special protocol. Telstra Big Pond protocol is used by the ISP in Australia. Your ISP should provide all the information required in this section. Please refer to section 4.2.6 for more settings of this option.



Telstra Big Pond (Australia Only)

If your Internet service is provided by Telstra Big Pond in Australia, you will need to enter your information below, This information is provided by Telstra BigPond.

User Name :

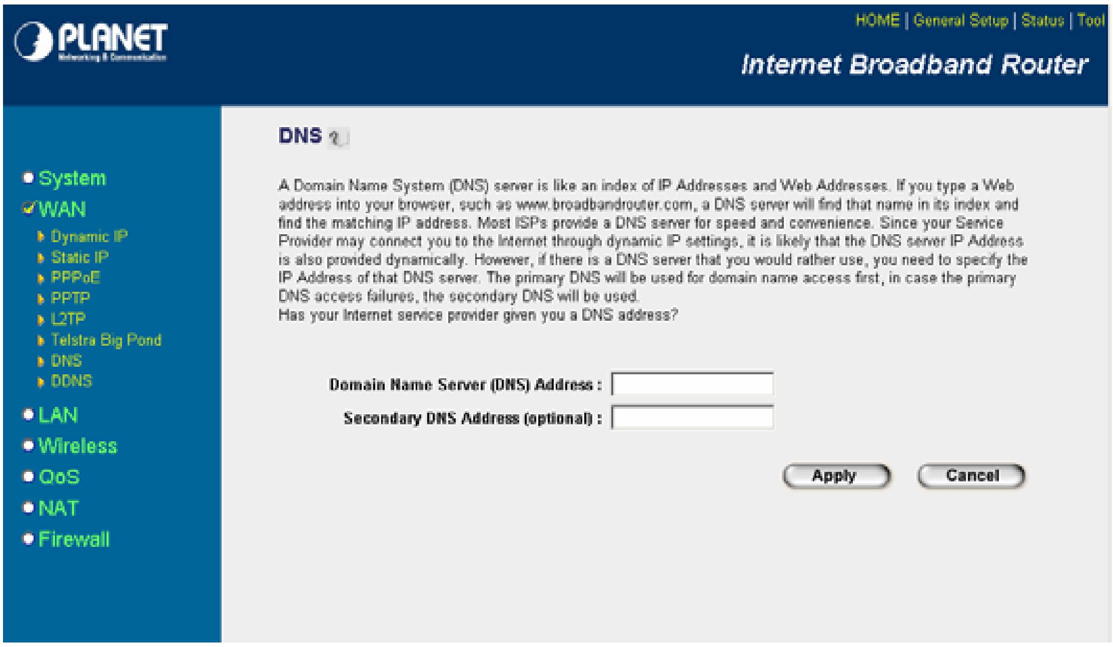
Password :

□ User decide login server manually

Login Server : 0.0.0.0

5.2.7 DNS

A Domain Name System (DNS) server is like an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.router.com, a DNS server will find that name in its index and the matching IP address. Most ISPs provide a DNS server for efficiency and convenience. If your Service Provider connects you to the Internet with dynamic IP settings, it is likely that the DNS server IP address is provided automatically. However, if there is a DNS server that you would rather to use, please specify the IP address of that DNS server here.



DNS

A Domain Name System (DNS) server is like an index of IP Addresses and Web Addresses. If you type a Web address into your browser, such as www.broadbandrouter.com, a DNS server will find that name in its index and find the matching IP address. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect you to the Internet through dynamic IP settings, it is likely that the DNS server IP Address is also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP Address of that DNS server. The primary DNS will be used for domain name access first, in case the primary DNS access failures, the secondary DNS will be used.
Has your Internet service provider given you a DNS address?

Domain Name Server (DNS) Address :

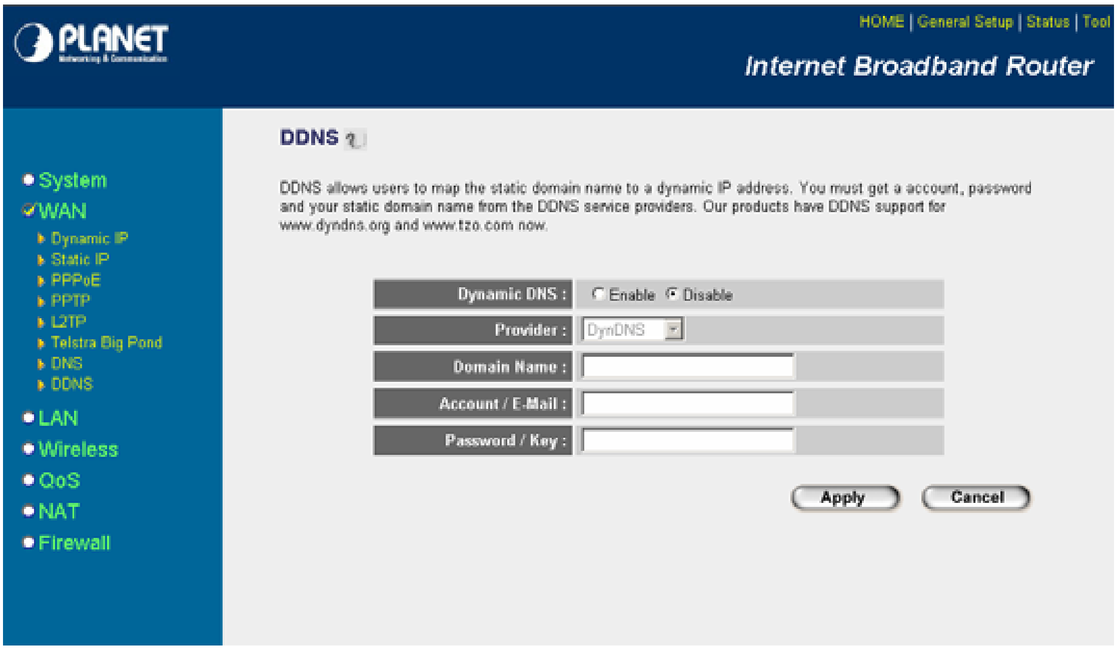
Secondary DNS Address (optional) :

Parameters	Description
Domain Name Server (DNS) Address	This is the ISP's DNS server IP address that they gave you; or you can specify your own preferred DNS server IP address.
Secondary DNS Address (optional)	This is optional. You can enter another DNS server's IP address as a backup. The secondary DNS will be used when the above primary DNS fails.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are saved successfully. You may press "Continue" for configure other settings or "Apply" to restart WMRT-414 with new configuration.

5.2.8 DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. This router supports DynDNS and TZO.



DDNS

DDNS allows users to map the static domain name to a dynamic IP address. You must get a account, password and your static domain name from the DDNS service providers. Our products have DDNS support for www.dyndns.org and www.tzo.com now.

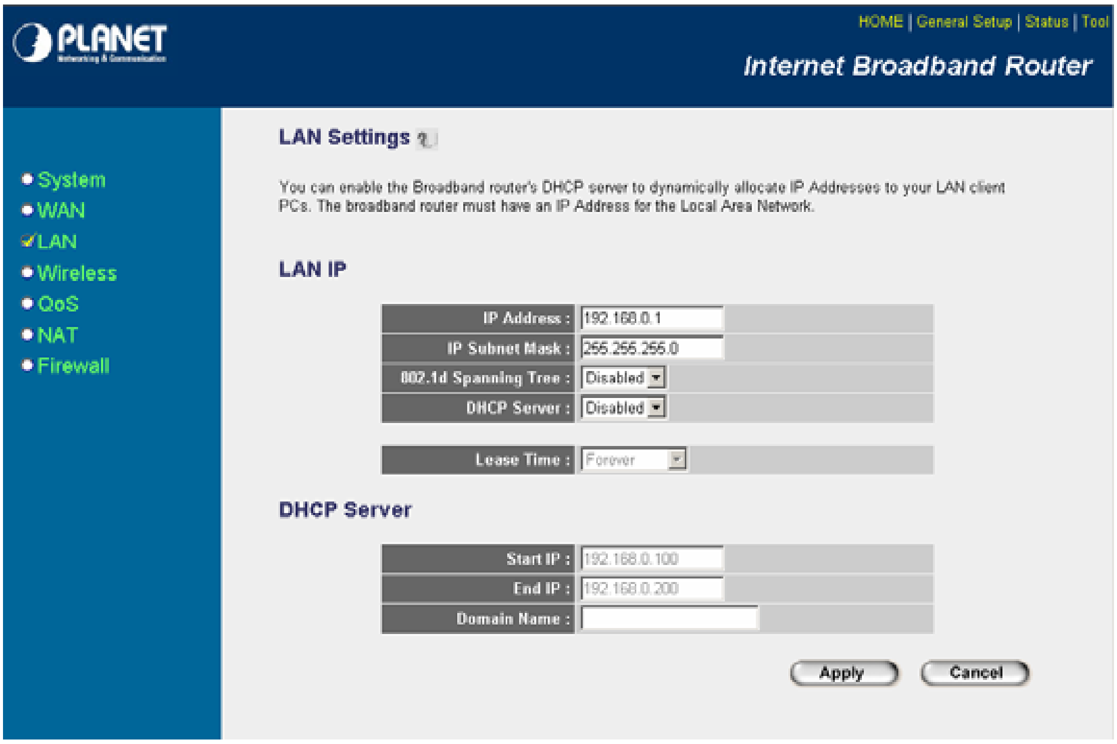
Dynamic DNS :	○ Enable ● Disable
Provider :	DynDNS
Domain Name :	
Account / E-Mail :	
Password / Key :	

Parameters	Description
Dynamic DNS	Enable/Disable the DDNS function of this router.
Provider	Select a DDNS service provider. The default setting is “DynDNS”.
Domain name	Your static domain name that use DDNS.
Account / E-mail	The account that your DDNS service provider assigned to you.
Password / Key	The password you set for the DDNS service account above.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

5.3 LAN

The LAN Port screen below allows you to specify a private IP address for your router's LAN interface.


PLANET
HOME | General Setup | Status | Tool
Internet Broadband Router
System
WAN
LAN
Wireless
QoS
NAT
Firewall
Apply
Cancel

LAN Settings

You can enable the Broadband router's DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The broadband router must have an IP Address for the Local Area Network.

LAN IP

IP Address : 192.168.0.1
IP Subnet Mask : 255.255.255.0
802.1d Spanning Tree : Disabled
DHCP Server : Disabled

Lease Time : Forever

DHCP Server

Start IP : 192.168.0.100
End IP : 192.168.0.200
Domain Name :

Parameters	**Description**
LAN IP	
IP Address	Designate the Access Point's IP Address. This IP Address should be unique in your network. The default IP Address is **192.168.0.1**.
Subnet Mask	Specify a Subnet Mask for your LAN segment. The Subnet Mask of the Access Point is fixed and the value is **255.255.255.0**.
802.1d Spanning Tree	If it is enabled, this router will use the spanning tree protocol to prevent from network loop happened in the LAN ports.
DHCP Server	Enable or disable the DHCP Server.
Lease Time	The DHCP Server will temporarily assign IP addresses to LAN clients. In the Lease Time setting you can specify the time period that the DHCP Server lends an IP address to your LAN client. The DHCP Server will change your LAN client's IP address when this time threshold period is reached.

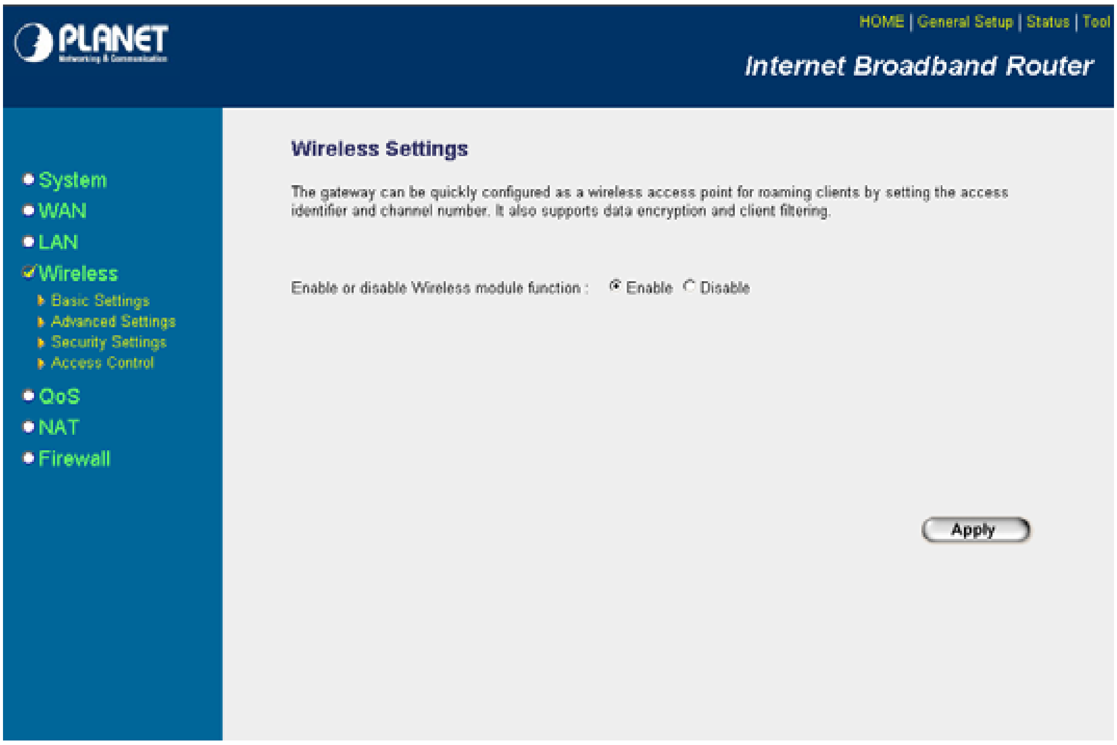
IP Address Pool	
Start IP/End IP	You can designate a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients. By default the IP range is from: Start IP **192.168.0.100** to End IP **192.168.0.200**.

Domain Name	You can specify the Domain Name for your Access Point.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

5.4 Wireless

This screen allows you to Enable/Disable WMRT-414 wireless function.



Wireless Settings

The gateway can be quickly configured as a wireless access point for roaming clients by setting the access identifier and channel number. It also supports data encryption and client filtering.

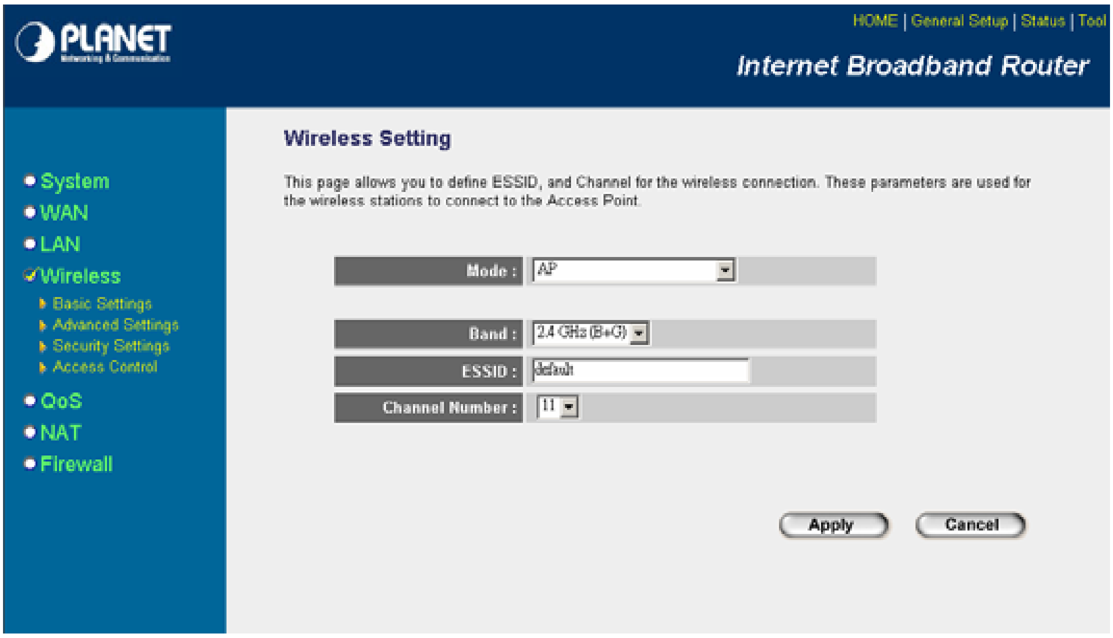
Enable or disable Wireless module function : ● Enable ○ Disable

Parameters	Description
Enable/Disable	You can select to “**Enable**” or “**Disable**” the Wireless interface. After selected, please click “Apply” to make the settings effect.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

5.4.1 Basic Settings

WMRT-414 supports not only Access Point function, but also provides Bridge and WDS mode. Please Refer to **"Chapter 6 Wireless Configuration**" know the details settings of wireless Basic Settings. In Default, WMRT-414 will work with AP mode.



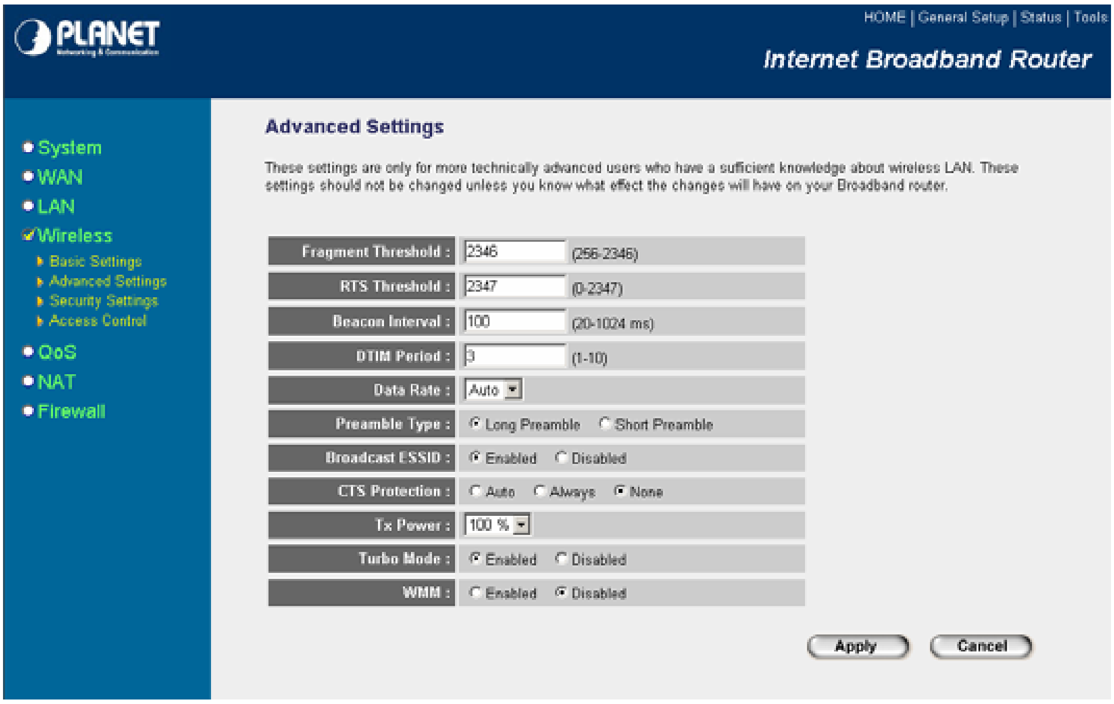
Wireless Setting

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode :	AP
Band :	2.4 GHz (B+G)
ESSID :	default
Channel Number :	11

5.4.2 Advance Settings

You should not change the parameters in this screen unless you know what effect the changes will have on WMRT-414. When configuration finished, please click "Apply" to save the settings.



Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router.

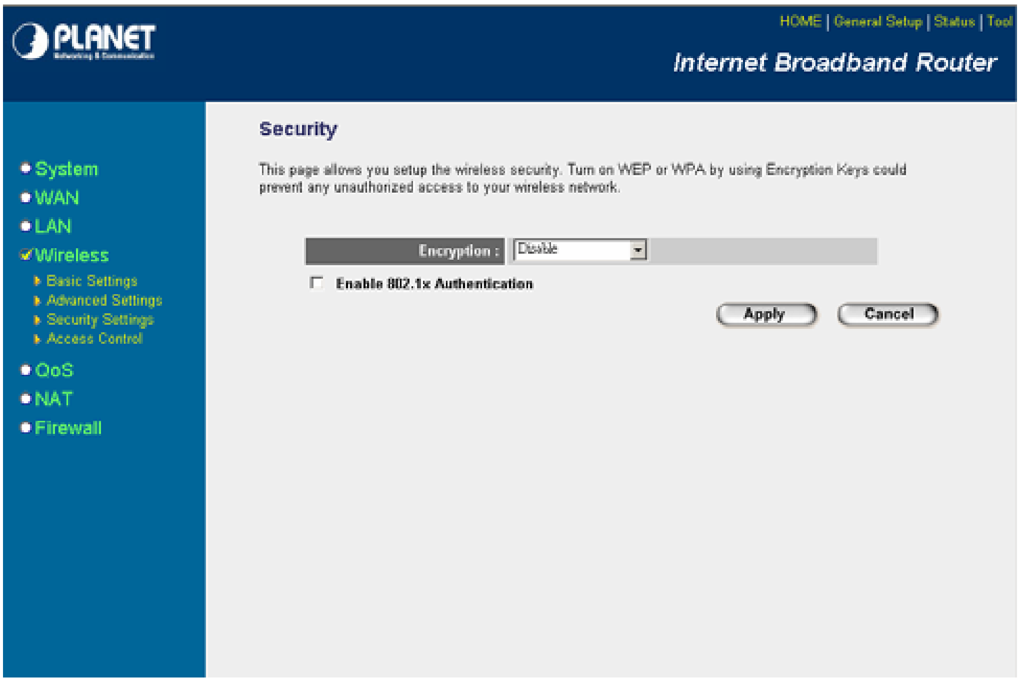
Fragment Threshold :	2346 (256-2346)
RTS Threshold :	2347 (0-2347)
Beacon Interval :	100 (20-1024 ms)
DTIM Period :	3 (1-10)
Data Rate :	Auto
Preamble Type :	● Long Preamble ○ Short Preamble
Broadcast ESSID :	● Enabled ○ Disabled
CTS Protection :	○ Auto ○ Always ● None
Tx Power :	100 %
Turbo Mode :	● Enabled ○ Disabled
WMM :	○ Enabled ● Disabled

Parameters	**Description**
Fragment Threshold	“Fragment Threshold” specifies the maximum size of packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.
RTS Threshold	When the packet size is smaller the RTS threshold, the access point will not use the RTS/CTS mechanism to send this packet.
Beacon Interval	The interval of time that this access point broadcast a beacon. Beacon is used to synchronize the wireless network.
Data Rate	The Data Rate is the rate of data transmission. The WMRT-414 will use the highest possible selected transmission rate to transmit the data packets.
Preamble Type	Preamble type defines the length of CRC block in the frames during the wireless communication. “**Short Preamble**” is suitable for high traffic wireless network. “**Long Preamble**” can provide more reliable communication.
Broadcast ESSID	If you enable “Broadcast ESSID”, every wireless station located within the coverage of this access point can discover this WMRT-414 easily. If you are building a public wireless network, enabling this feature is recommended. In private network, disabling “Broadcast ESSID” can provide better security.
CTS Protection	It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to many of frame traffic should be transmitted.
TX Power	Users can adjust the WMRT-414 output power to 100%, 90%, 75% 50% 25% and 10%. In default, WMRT-414 will work with 100% output power.
Turbo Mode	Enable/Disable Turbo mode. When the connect client has support Turbo mode also, they can work with better performance.
WMM	Enable/Disable WMM function.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

5.4.3 Security

WMRT-414 provides complete wireless LAN security functions, includes WEP, 802.1x, 802.1x with WEP, WPA-PSK and WPA RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function. In default, the security function is “Disable”.



Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

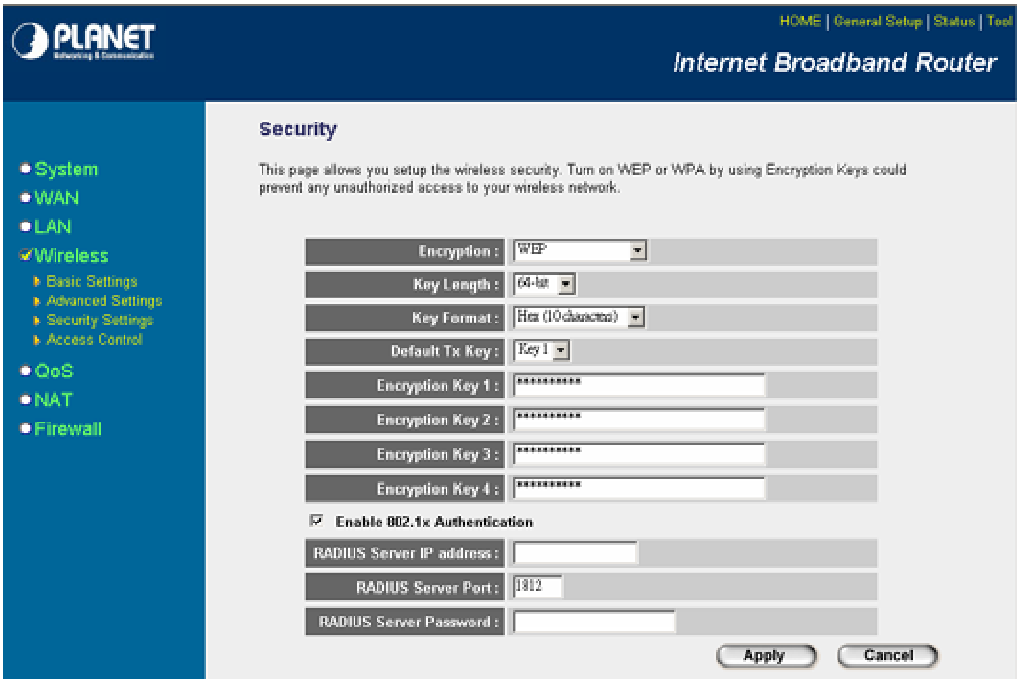
Encryption :	Disable

□ Enable 802.1x Authentication

5.4.3.1 WEP

When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself. You can enter four WEP keys and select one of them as default key. Then the access point will just allow the clients that with the same encryption keys connected. You can use WEP encryption in “AP mode”, “Station-Ad Hoc mode”, “Station-Infrastructure mode” and “AP Bridge-WDS mode”.

If you would like to enable 802.1x Authentication also, please check the “Enable 802.1x Authentication” and refer to section 5.4.3.2 for the detail of 802.1x settings.



Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption :	WEP
Key Length :	64-bit
Key Format :	Hex (10 characters)
Default Tx Key :	Key 1
Encryption Key 1 :	**********
Encryption Key 2 :	**********
Encryption Key 3 :	**********
Encryption Key 4 :	**********

☑ Enable 802.1x Authentication

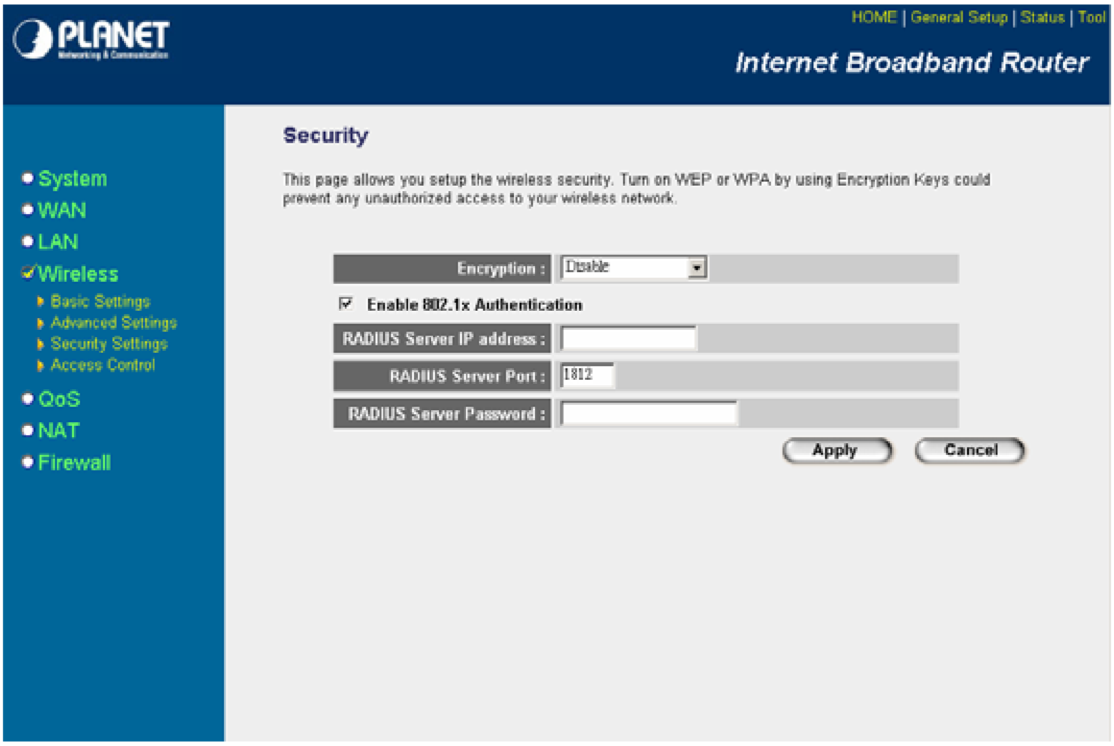
RADIUS Server IP address :	
RADIUS Server Port :	1812
RADIUS Server Password :	

Parameter	Description
Encryption	Please select “WEP” in this option.
Key Length	You can select the 64 or 128-bit key to encrypt transmitted data. Larger WEP key length will provide higher level of security, but the throughput will be lower.
Key Format	You may select to select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the WEP Key.
Default Tx Key	Select one of the four keys to encrypt your data. Only the key you select it in the “Default key” will take effect.
Encryption Key 1 - Key 4	The WEP keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. 64-bit WEP: input 10-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 10-digit ASCII characters as the encryption keys.
Enable 802.1x Authentication	Check this box if you want to enable 802.1x authentication with WEP encryption. You may refer to section 5.4.3.2 to enter the correct setting of the fields.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

5.4.3.2 802.1x

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encryption the data during communication. It is suggested to enable 802.1x and WEP at the same time.



Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption : Disable

☑ Enable 802.1x Authentication

RADIUS Server IP address :

RADIUS Server Port : 1812

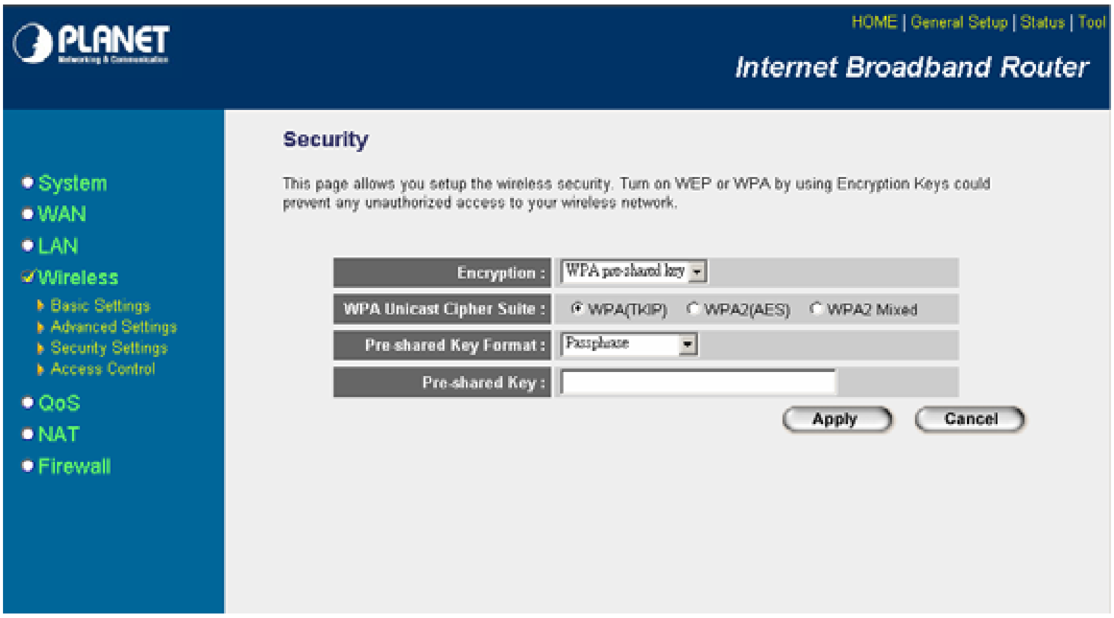
RADIUS Server Password :

Parameter	Description
Encryption	If you want to use 802.1x only, keep this setting in “Disable”.
Enable 802.1x Authentication	Please check this option to enable 802.1x function.
RADIUS Server IP Address	Enter RADIUS Serer IP address.
RADIUS Server Port	Leave the default port setting or assign a new port number for this option.
RADIUS Server Password	Please enter the password that is configured in RADIUS Server.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

5.4.3.3 WPA-PSK

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be broken by hackers. This can improve security very much.



Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption : WPA pre-shared key

WPA Unicast Cipher Suite : ● WPA(TKIP) ○ WPA2(AES) ○ WPA2 Mixed

Pre-shared Key Format : Passphrase

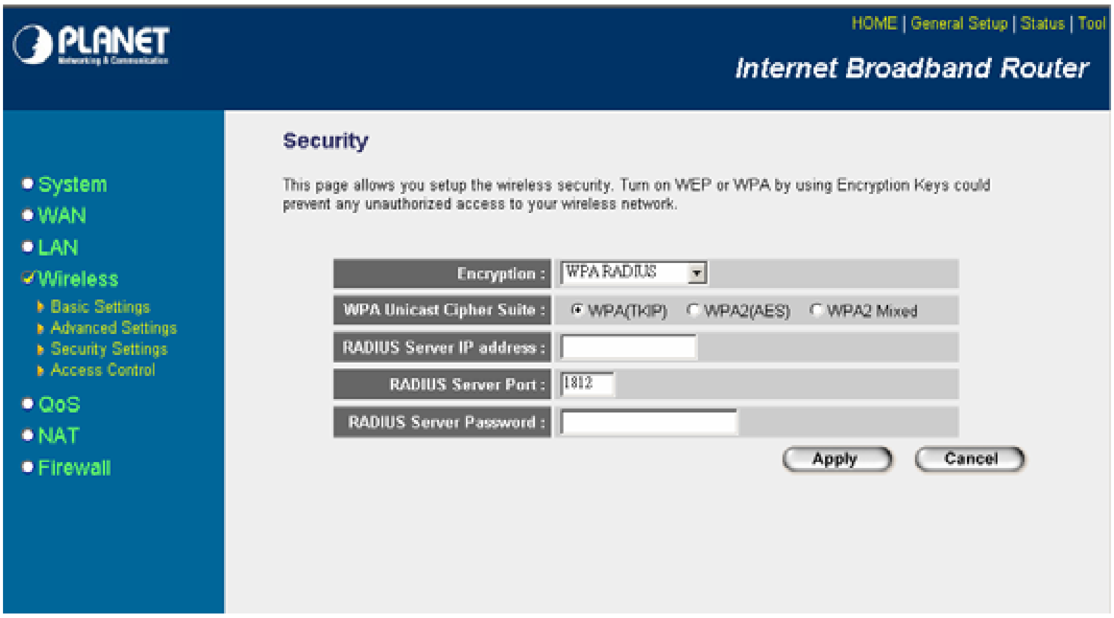
Pre-shared Key :

Parameter		**Description**
Encryption		Please select “WPA pre-shared key” in this option.
WPA Unicast Cipher Suite	WPA (TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
	WPA2 (AES)	This use CCMP protocol to change encryption key frequently. AES can provide high-level encryption to enhance the wireless LAN security.
	WPA2 Mixed	This will use TKIP or AES based on the other communication peer automatically.
Pre-shared Key Format		You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the Pre-shared Key.
Pre-shared Key		The Pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill the text box by following the rules below. Hex: input 64-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or at least 8 character pass phrase as the pre-shared keys.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

5.4.3.4 WPA RADIUS

You can use a RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently.



Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption : WPA RADIUS

WPA Unicast Cipher Suite : ● WPA(TKIP) ○ WPA2(AES) ○ WPA2 Mixed

RADIUS Server IP address :

RADIUS Server Port : 1812

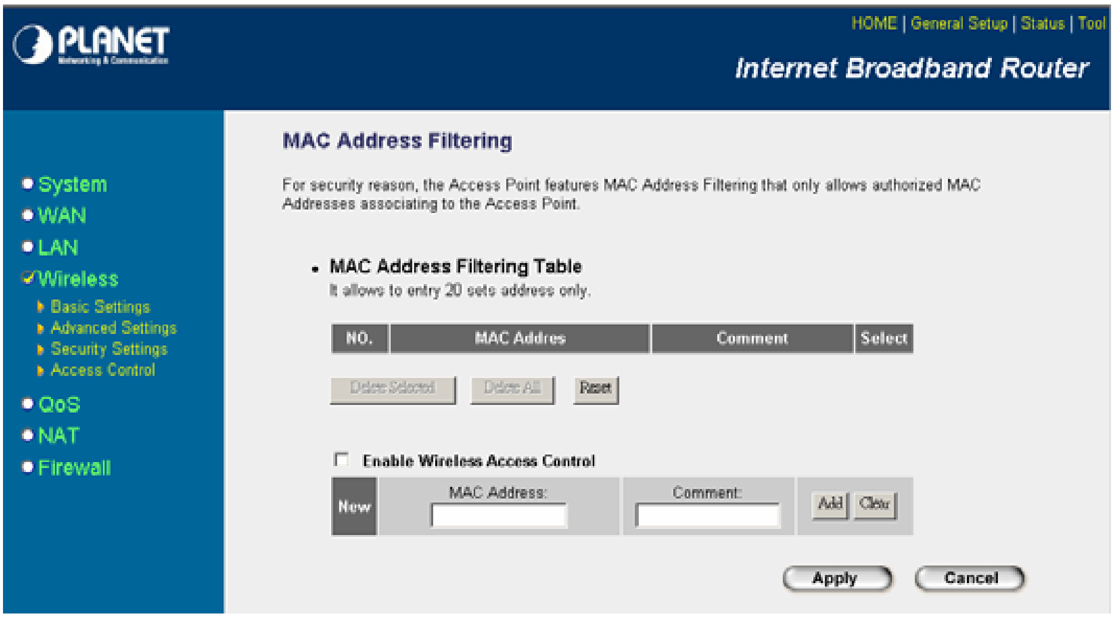
RADIUS Server Password :

Parameter		**Description**
Encryption		Please select “WPA RADIUS” in this option.
WPA Unicast Cipher Suite	WPA (TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
	WPA2 (AES)	This use CCMP protocol to change encryption key frequently. AES can provide high-level encryption to enhance the wireless LAN security.
	WPA2 Mixed	This will use TKIP or AES based on the other communication peer automatically.
RADIUS Server IP Address		Enter RADIUS Serer IP address.
RADIUS Server Port		Leave the default port setting or assign a new port number for this option.
RADIUS Server Password		Please enter the password that is assigned in RADIUS Server.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

5.4.4 Access Control

WMRT-414 provides MAC Address Filtering, which prevents the unauthorized users from accessing your wireless network.



MAC Address Filtering

For security reason, the Access Point features MAC Address Filtering that only allows authorized MAC Addresses associating to the Access Point.

- MAC Address Filtering Table

It allows to entry 20 sets address only.

NO.	MAC Addres	Comment	Select

□ Enable Wireless Access Control

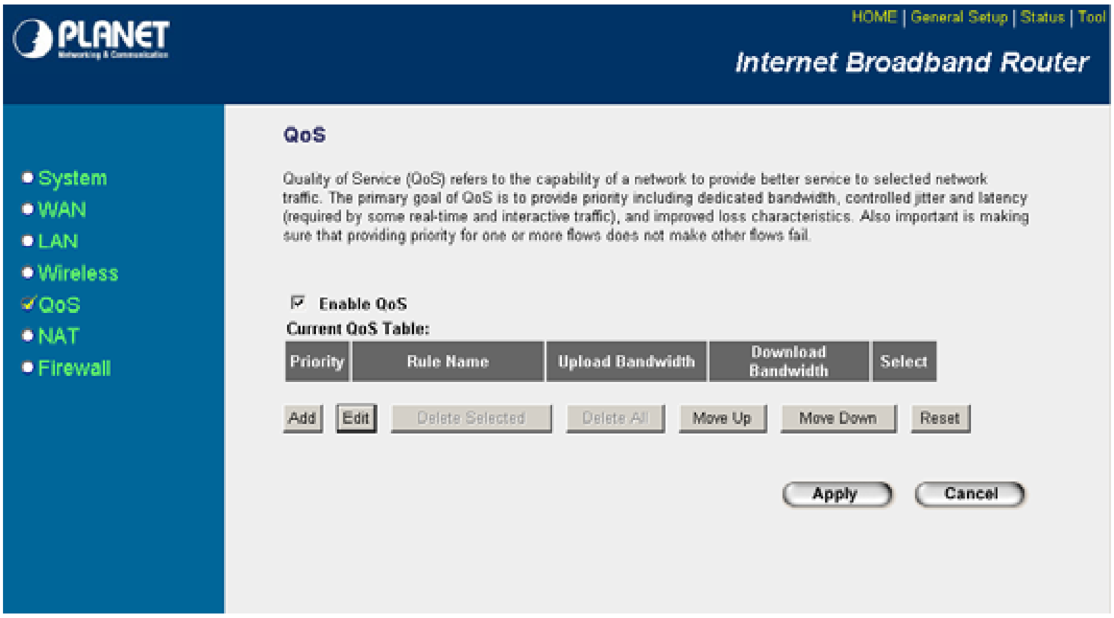
New MAC Address: Comment:

Parameters	Description
Enable Wireless Access Control	Enable or disable the MAC Address Filtering function.
Add MAC Address to the control table	In the bottom “New” area, fill in the “MAC Address” and “Comment” of the wireless station and then click “Add”. Then this wireless station will be added into the “MAC Address Filtering Table” above.
Remove MAC address from the table	If you want to remove some MAC address from the “Current Access Control List”, select the MAC addresses you want to remove in the list and then click “Delete Selected”.
Delete All	If you want remove all MAC addresses from the list, just click this button.
Reset	Click “Reset” will clear your current selections.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

5.5 QoS

Quality of Service (QoS) refers to the capability of providing better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. When using this feature, it is important to make sure the rules are not conflicted with each other.



QoS

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail.

☑ Enable QoS

Current QoS Table:

Priority	Rule Name	Upload Bandwidth	Download Bandwidth	Select

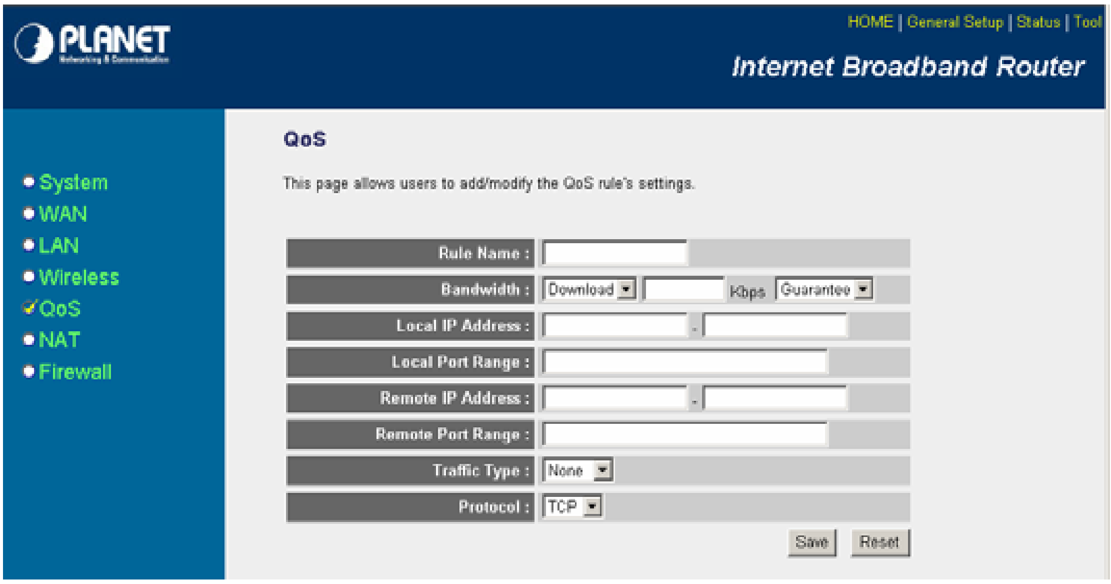
Parameters	Description
Add	When you want to add a new QoS rule, press this button and refer to section 5.5.1 to add a new QoS rule.
Edit	When you want to edit the existing QoS rule, press this button and refer to section 5.5.1 to edit QoS rule.
Delete Selected	Select the QoS rule which you would like to delete , then press this button to delete.
Delete All	When you want to delete all the QoS rules, you just need to press this button.
Move Up	Select a QoS rule and press this button to assign higher priority.
Remove Down	Select a QoS rule and press this button to assign lower priority.
Reset	Click “Reset” to clear your current selections.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

5.5.1 Add/Edit QoS Rule

You can assign packet classification criteria by its source IP range, destination IP range, traffic type, protocol, source port range and destination port range parameters. The parameters that you leave as blank will be ignored. The priority of this rule will be applied to packets that match classification criteria of this rule. You can limit bandwidth consumed by packets that match this rule or guarantee bandwidth required by packets that match this rule.

After press Add or Edit button in QoS screen, you will see the web screen below for user to setup their QoS rule.



PLANET
HOME | General Setup | Status | Tool
Internet Broadband Router
System
WAN
LAN
Wireless
QoS
NAT
Firewall

QoS

This page allows users to add/modify the QoS rule's settings.

Rule Name :	
Bandwidth :	Download ▾ Kbps Guarantee ▾
Local IP Address :	-
Local Port Range :	
Remote IP Address :	-
Remote Port Range :	
Traffic Type :	None ▾
Protocol :	TCP ▾

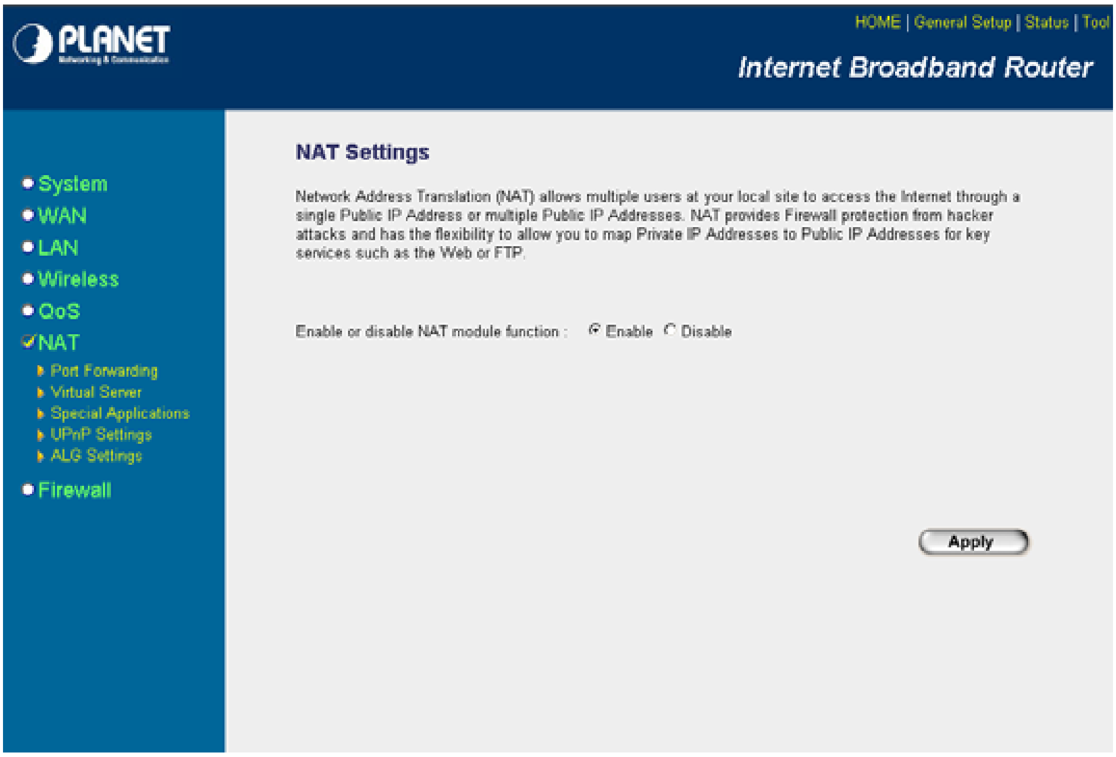
Parameters	Description
Rule Name	Please give a name to the QoS Rule
Bandwidth	You can limit the maximum bandwidth consumed by this rule by selecting "Maximum". You also can reserve enough bandwidth for this rule by selecting "Guarantee". The unit of bandwidth is Kbps. When we download data from Internet, the unit of download screen shows is KBps. 1KBps is equal to 8Kbps. When you enter the bandwidth, please make sure the number you enter is correct. For example, if you want to limit users download speed to 50KBps from Internet, you will need to enter 400Kbps in the configuration.
Local IP Address	Please enter the IP address of the local PC.
Local Port Range	Please enter the port range.
Remote IP Address	Please enter the IP address of the PC from remote site.
Remote Port Range	Please enter the port range.
Traffic Type	Select the traffic type of the packets that this rule will apply to. We list some popular applications here to ease the configuration. You also can get the same result by using other parameters, for example source or destination

	port number, if you are familiar with the application protocol.
Protocol	Please select the protocol TCP or UDP in the list.

After configuration complete, please click “Save” to save the settings. Or you may press “Reset” to clear the settings to enter again.

5.6 NAT

Network Address Translation (NAT) allows multiple users at your local site to access the Internet via a single legal IP Address. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP. If NAT is disabled, all LAN side workstations must have legal IP addresses for Internet access. If the router is used for routing application, not for Internet access, the NAT function can be disabled.



NAT Settings

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as the Web or FTP.

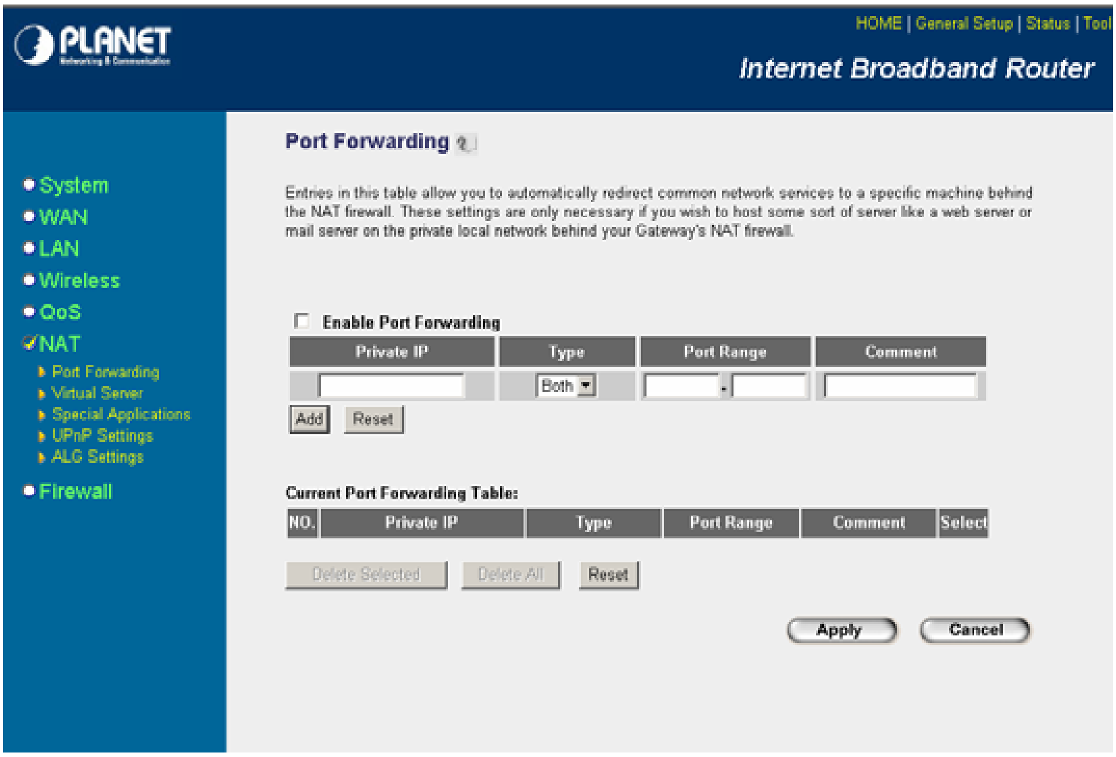
Enable or disable NAT module function : ● Enable ○ Disable

Parameters	Description
Enable/Disable	You can select to enable or disable the NAT function. After selected, please click “Apply” to make the settings effect.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

5.6.1 Port Forwarding

The Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address. It helps you to host some servers behind the firewall.



Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

□ Enable Port Forwarding

Private IP	Type	Port Range	Comment
	Both	-	

Current Port Forwarding Table:

NO.	Private IP	Type	Port Range	Comment	Select

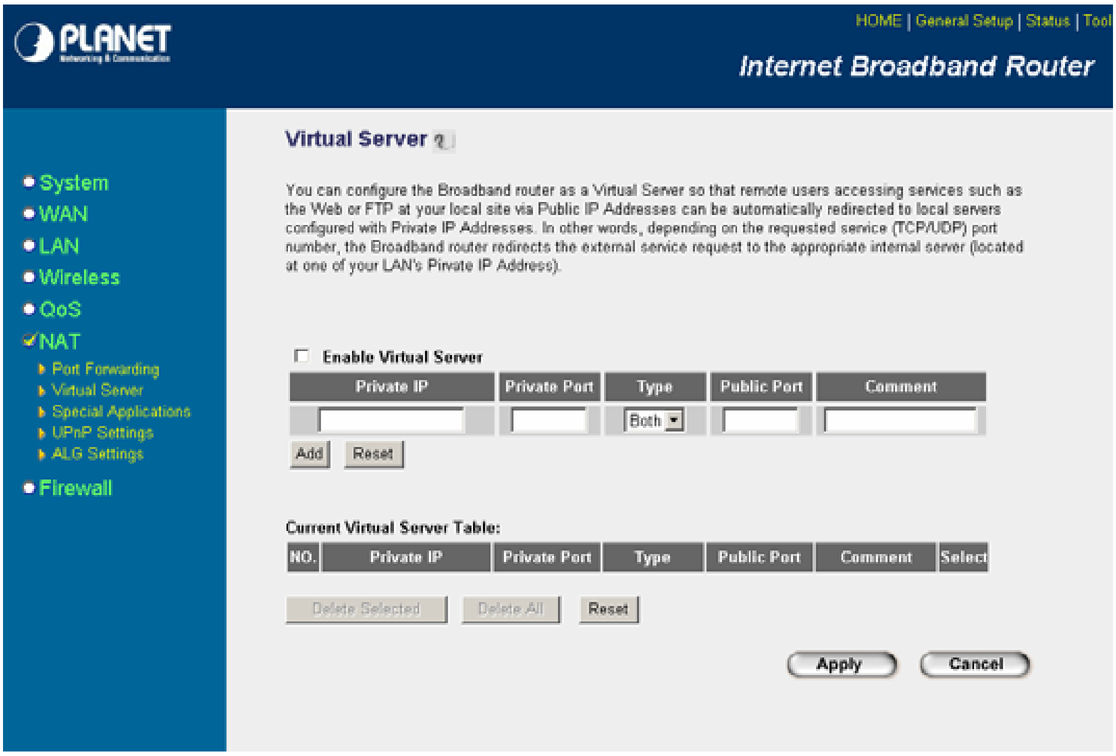
Parameters	Description
Enable Port Forwarding	Enable Port Forwarding.
Private IP	This is the private IP of the server in LAN. **Note:** You need to give your LAN PC clients a fixed/static IP address for Port Forwarding to work properly.
Type	This is the protocol type to be forwarded. You can choose to forward “TCP” or “UDP” packets only or select “both” to forward both “TCP” and “UDP” packets.
Port Range	The range of ports to be forward to the private IP.
Comment	The description of this setting.
Add	Fill in the "Private IP", “Type”, “Port Range” and "Comment" of the setting to be added and then click "Add". Then this Port Forwarding setting will be added into the "Current Port Forwarding Table" below. If you find any typo before adding it and want to retype again, just click "Clear" and the fields will be cleared.
Reset	Click “Reset” will clear your current settings to allows you to enter again.

Current Port Forwarding Table	
Delete Selected	If you want to remove some MAC address from the "Current Access Control List", select the MAC addresses you want to remove in the table and then click "Delete Selected".
Delete All	If you want remove all MAC addresses from the table, just click this button.
Reset	Click "Reset" will clear your current selections.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press "Continue" for configure other settings or "Apply" to restart WMRT-414 with new configuration.

5.6.2 Virtual Server

Use the Virtual Server function when you need to have different servers in your LAN to handle many services and Internet applications (e.g. Email, FTP, Web server etc.) to the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to re-direct a particular service port number (from the WAN Port) to a particular LAN private IP address as its service port number. (See Glossary for an explanation on Port number).



Virtual Server

You can configure the Broadband router as a Virtual Server so that remote users accessing services such as the Web or FTP at your local site via Public IP Addresses can be automatically redirected to local servers configured with Private IP Addresses. In other words, depending on the requested service (TCP/UDP) port number, the Broadband router redirects the external service request to the appropriate internal server (located at one of your LAN's Private IP Address).

☐ Enable Virtual Server

Private IP	Private Port	Type	Public Port	Comment
		Both		

Current Virtual Server Table:

NO.	Private IP	Private Port	Type	Public Port	Comment	Select

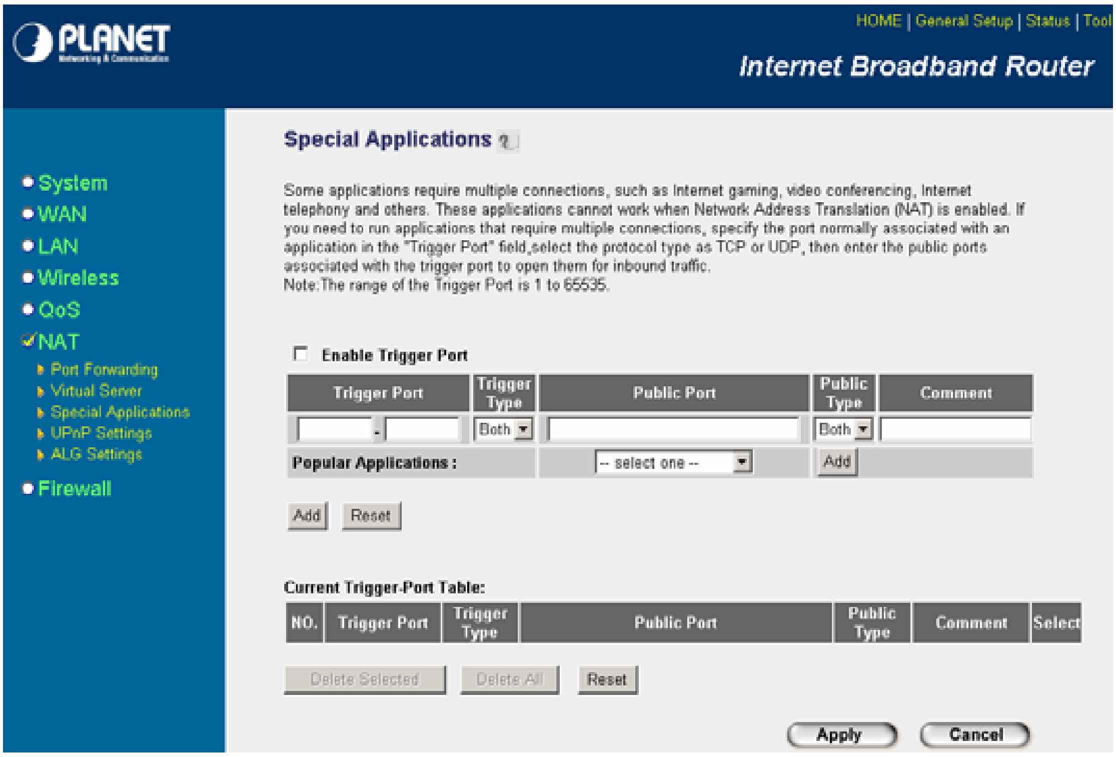
Parameters	**Description**
Enable Virtual Server	Enable Virtual Server.
Private IP	This is the LAN client/host IP address that the Public Port number packet will be sent to.

	Note: You need to give your LAN PC clients a fixed/static IP address for Virtual Server to work properly.
Private Port	This is the port number (of the above Private IP host) that the below Public Port number will be changed to when the packet enters your LAN (to the LAN Server/Client IP).
Type	Select the port number protocol type (**TCP**, **UDP** or **Both**). If you are unsure, then leave it to the default both protocols.
Public Port	Enter the service (service/Internet application) port number from the Internet that will be re-directed to the above Private IP address host in your LAN. **Note:** Virtual Server function will have priority over the DMZ function if there is a conflict between the Virtual Server and the DMZ settings.
Add	Fill in the "Private IP", "Private Port", "Type", “Public Port” and "Comment" of the setting to be added and then click "Add". Then this Virtual Server setting will be added into the "Current Virtual Server Table" below. If you find any typo before adding it and want to retype again, just click "Clear" and the fields will be cleared.
Reset	Click “Reset” will clear your current settings to allows you to enter again.
Current Virtual Server Table	
Delete Selected	If you want to remove some items from the “Current Virtual Server Table”, select the MAC addresses you want to remove in the table and then click “Delete Selected”.
Delete All	If you want remove all items of the table, just click this button.
Reset	Click “Reset” will clear your current selections.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

5.6.3 Special Applications

Some applications require multiple connections, such as Internet games, video conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.



Special Applications

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field,select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.
Note:The range of the Trigger Port is 1 to 65535.

☐ Enable Trigger Port

Trigger Port	Trigger Type	Public Port	Public Type	Comment
-	Both		Both	
Popular Applications :		-- select one --	Add	

Current Trigger-Port Table:

NO.	Trigger Port	Trigger Type	Public Port	Public Type	Comment	Select

Parameters	Description
Enable Trigger Port	Enable the Special Application function.
Trigger Port	This is the out going (Outbound) range of port numbers for this particular application.
Trigger Type	Select whether the outbound port protocol are “**TCP**”, “**UDP**” or “**Both**”.
Public Port	Enter the In-coming (Inbound) port or port range for this type of application (e.g. 2300-2400, 47624). **Note:** Individual port numbers are separated by a comma (e.g. 47624, 5775, 6541 etc.). To input a port range use a “dash” to separate the two port number range (e.g. 2300-2400).
Public Type	Select the Inbound port protocol type: “TCP”, “UDP” or both.
Comment	The description of this setting.
Popular applications	This section lists the more popular applications that require multiple connections. Select an application from the Popular Applications selection. Once you have selected an application, click the “Add” button in right side of this setting. This will automatically copy the Port Trigger information required

	for this popular application into the input fields.
Add	Add the settings into the “Current Trigger Port Table”.
Reset	Click “Reset” will clear your current settings to allows you to enter again.
Current Trigger Port Table	
Delete Selected	If you want to remove some items from the “Current Trigger Port Table”, select the MAC addresses you want to remove in the table and then click “Delete Selected”.
Delete All	If you want to remove all items from the table, just click this button.
Reset	Click “Reset” will clear your current selections.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

Example: Special Applications

If you need to run applications that require multiple connections, specify the port (outbound) normally associated with that application in the "Trigger Port" field. Then select the protocol type (TCP or UDP) and enter the public ports associated with the trigger port to open them up for inbound traffic.

Example:

ID	Trigger Port	Trigger Type	Public Port	Public Type	Comment
1	28800	UDP	2300-2400, 47624	TCP	MSN Game Zone
2	6112	UDP	6112	UDP	Battle.net

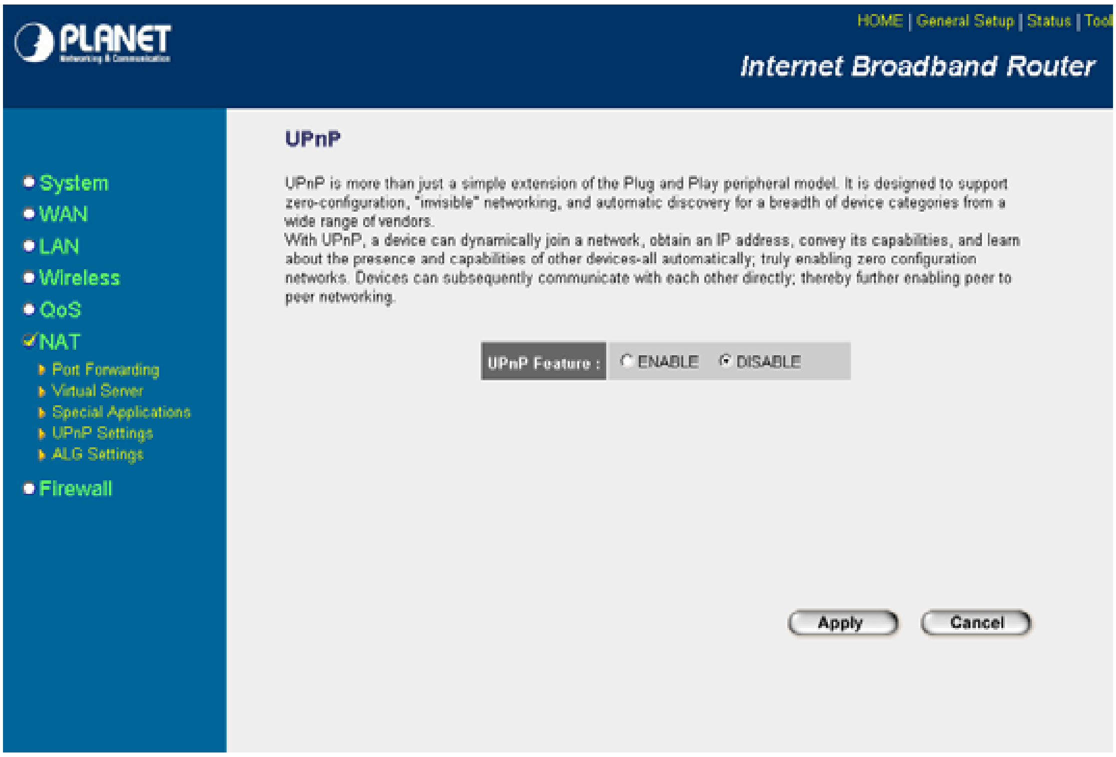
In the example above, when a user trigger’s port 28800 (outbound) for MSN Game Zone then the router will allow incoming packets for ports 2300-2400 and 47624 to be directed to that user.

Note: Only one LAN client can use a particular special application at a time.

5.6.4 UPnP

UPnP is more than just a simple extension of the Plug and Play peripheral model. It is designed to support zero-configuration, "invisible" networking, and automatic discovery for a breadth of device categories from a wide range of vendors.

With UPnP, a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices-all automatically; truly enabling zero configuration networks. Devices can subsequently communicate with each other directly; thereby further enabling peer to peer networking.



UPnP

UPnP is more than just a simple extension of the Plug and Play peripheral model. It is designed to support zero-configuration, "invisible" networking, and automatic discovery for a breadth of device categories from a wide range of vendors.
With UPnP, a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices-all automatically; truly enabling zero configuration networks. Devices can subsequently communicate with each other directly; thereby further enabling peer to peer networking.

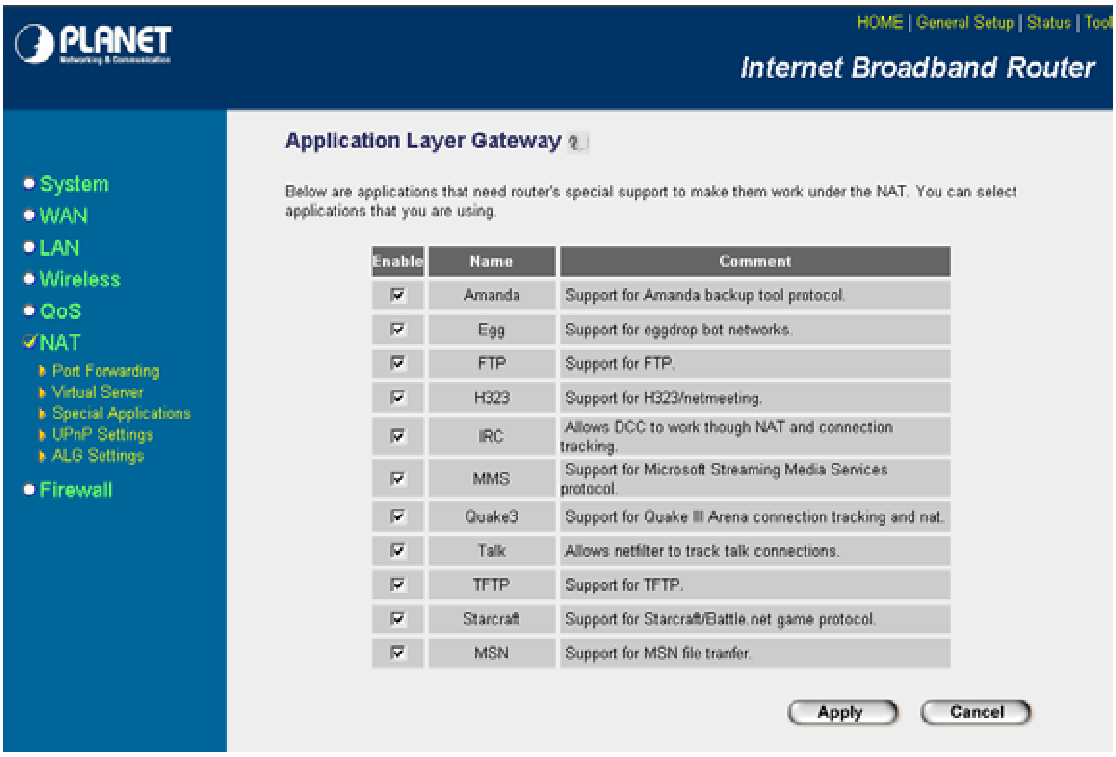
UPnP Feature : ○ ENABLE ● DISABLE

Parameters	Description
UPnP Feature	Enable or Disable UPnP function.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

5.6.5 ALG Settings

You can select applications that need “Application Layer Gateway” to support.



Application Layer Gateway

Below are applications that need router's special support to make them work under the NAT. You can select applications that you are using.

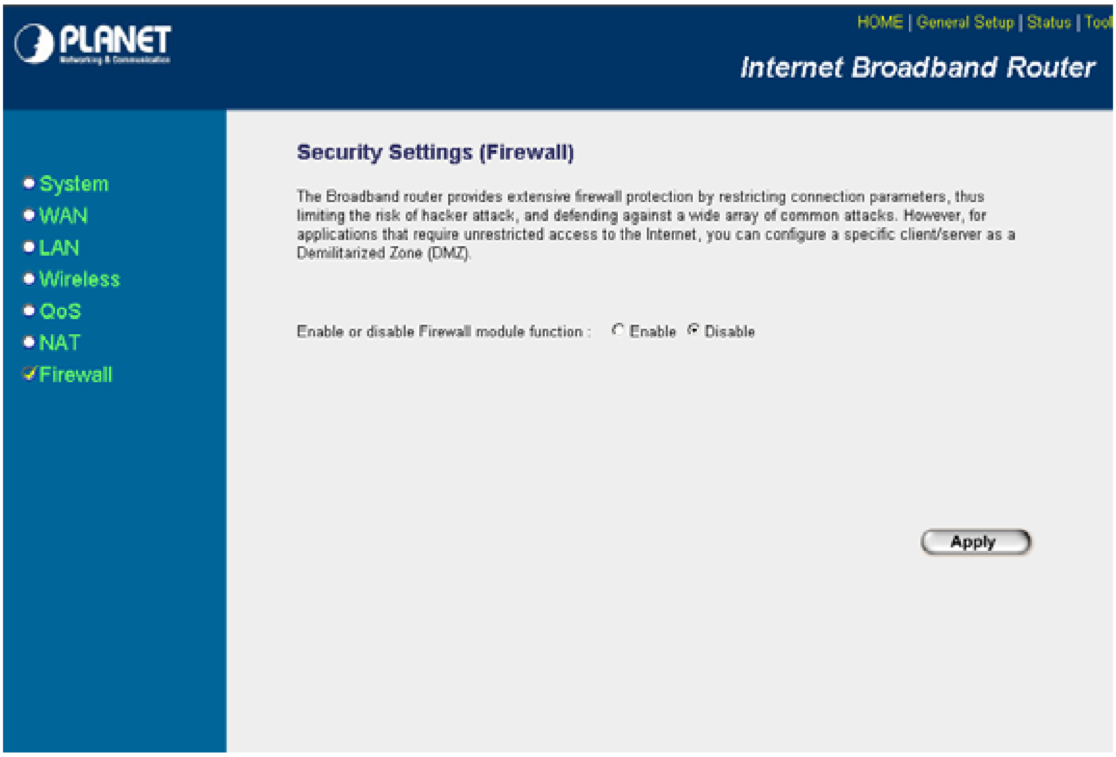
Enable	Name	Comment
☑	Amanda	Support for Amanda backup tool protocol.
☑	Egg	Support for eggdrop bot networks.
☑	FTP	Support for FTP.
☑	H323	Support for H323/netmeeting.
☑	IRC	Allows DCC to work though NAT and connection tracking.
☑	MMS	Support for Microsoft Streaming Media Services protocol.
☑	Quake3	Support for Quake III Arena connection tracking and nat.
☑	Talk	Allows netfilter to track talk connections.
☑	TFTP	Support for TFTP.
☑	Starcraft	Support for Starcraft/Battle.net game protocol.
☑	MSN	Support for MSN file tranfer.

Parameters	Description
Enable	You can select to enable “Application Layer Gateway” of an application and then the router will let that application correctly pass though the NAT gateway.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

5.7 Firewall

WMRT-414 provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server in a Demilitarized Zone (DMZ).


PLANET
Networking & Communication
HOME | General Setup | Status | Tool
Internet Broadband Router
System
WAN
LAN
Wireless
QoS
NAT
Firewall
Apply

Security Settings (Firewall)

The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

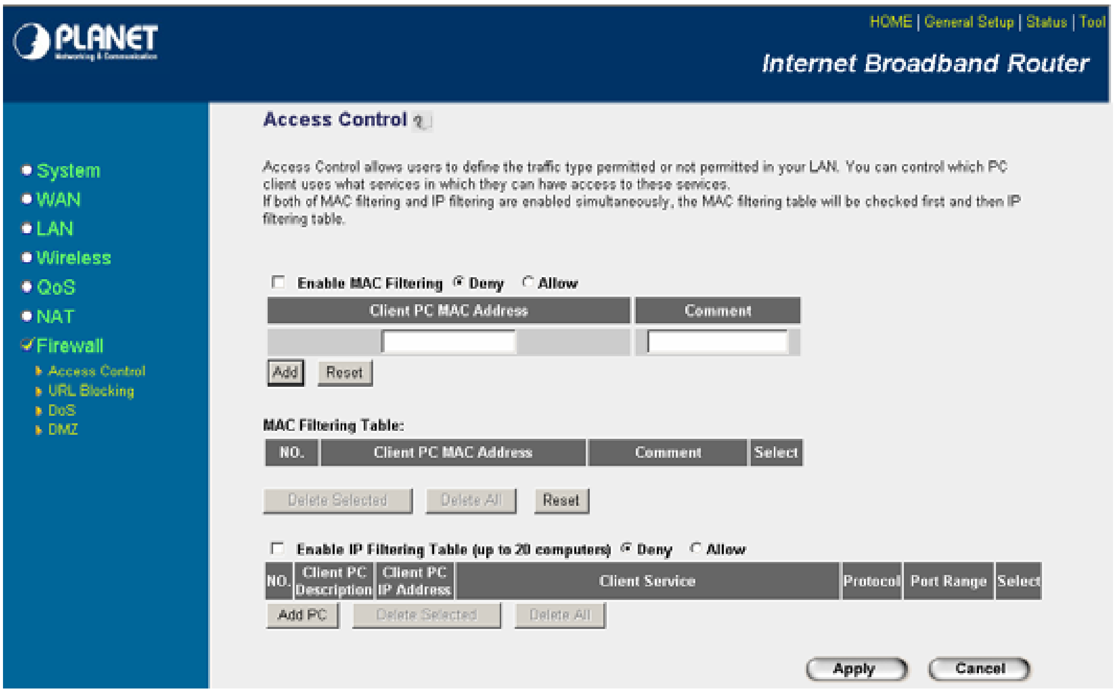
Enable or disable Firewall module function : ○ Enable ● Disable

Parameters	**Description**
Enable/Disable	You can select to enable or disable the firewall function. After selected, please click "Apply" to make the settings effect.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press "Continue" for configure other settings or "Apply" to restart WMRT-414 with new configuration.

5.7.1 Access Control

This screen allows you to restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.). Network administrator can define the traffic type permitted in your LAN and control which PC client can have access to these services.


PLANET
Networking & Communication
HOME | General Setup | Status | Tool
Internet Broadband Router
System
WAN
LAN
Wireless
QoS
NAT
Firewall
Access Control
URL Blocking
DoS
DMZ

Access Control

Access Control allows users to define the traffic type permitted or not permitted in your LAN. You can control which PC client uses what services in which they can have access to these services.
If both of MAC filtering and IP filtering are enabled simultaneously, the MAC filtering table will be checked first and then IP filtering table.

□ Enable MAC Filtering ● Deny ○ Allow

Client PC MAC Address	Comment

MAC Filtering Table:

NO.	Client PC MAC Address	Comment	Select

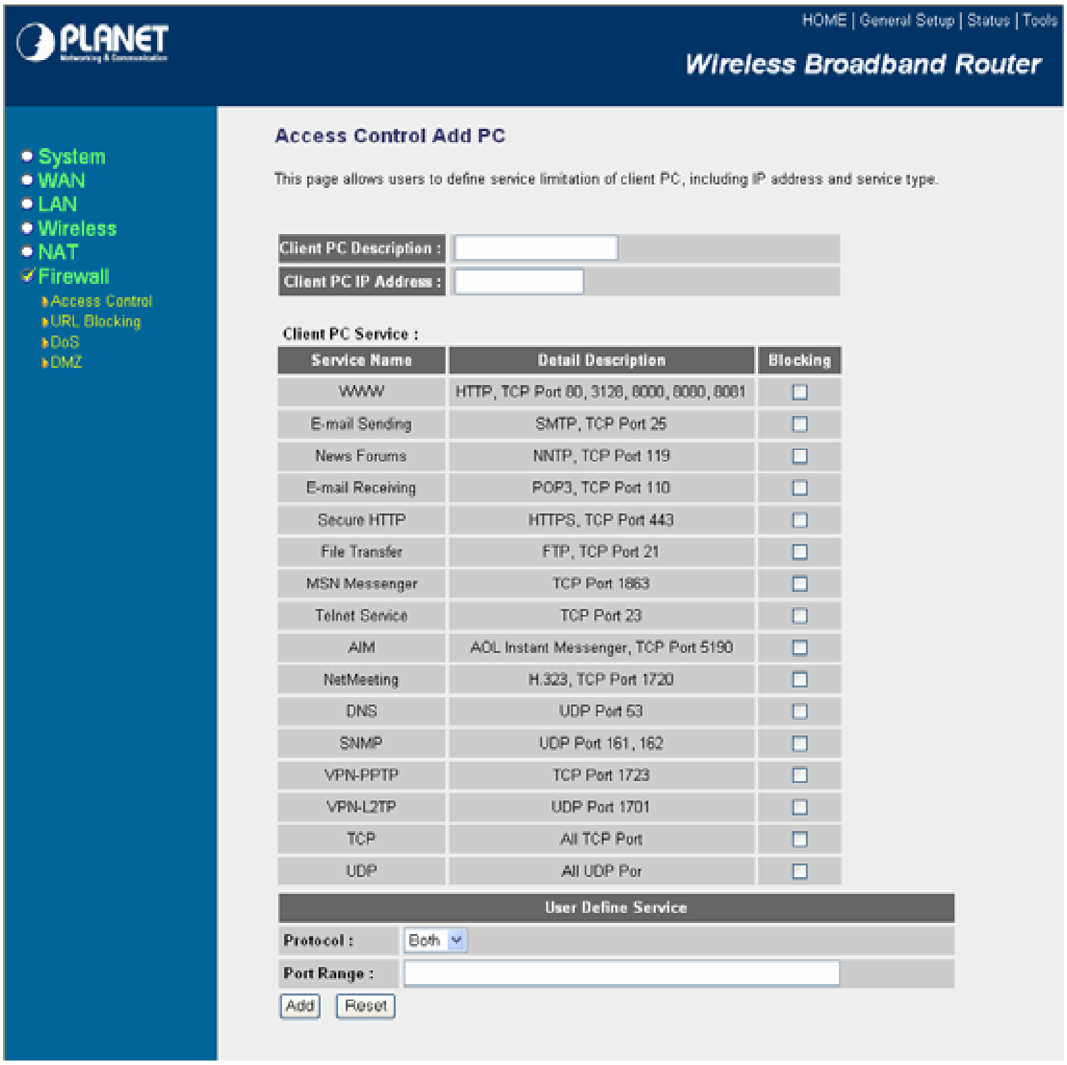
□ Enable IP Filtering Table (up to 20 computers) ● Deny ○ Allow

NO.	Client PC Description	Client PC IP Address	Client Service	Protocol	Port Range	Select

Parameters	Description
Enable MAC Filtering	Check “Enable MAC Filtering” to enable MAC Filtering. If select “Deny”, all PCs will be allowed to access Internet accept for the PCs in the list below. If select “Allow”, all PCs will be denied to access Internet accept for the PCs in the list below.
Add PC	Fill in “Client PC MAC Address” and “Comment” of the PC that is allowed to access the Internet, and then click “Add”. If you find any typo before adding it and want to retype again, just click "Reset" and the fields will be cleared.
Remove PC	If you want to remove some PC from the "MAC Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want remove all PCs from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click “Reset”.
Enable IP Filtering Table	Check “Enable IP Filtering Table” to enable IP filter. If select “Deny”, all PCs will be allowed to access Internet accept for the PCs in the list below. If select “Allow”, all PCs will be denied to access Internet accept for the PCs

	in the list below.
Add PC	You can click “Add PC” to add an access control rule for users by IP addresses. Please refer to section 5.7.1.1.
Remove PC	If you want to remove some PCs from the "IP Filtering Table", select the PC you want to remove in the table and then click "Delete Selected".
Delete All	If you want to delete all PCs. Please click this button.

5.7.1.1 Add PC



Access Control Add PC

This page allows users to define service limitation of client PC, including IP address and service type.

Client PC Description :	
Client PC IP Address :	

Client PC Service :

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8080, 8081	□
E-mail Sending	SMTP, TCP Port 25	□
News Forums	NNTP, TCP Port 119	□
E-mail Receiving	POP3, TCP Port 110	□
Secure HTTP	HTTPS, TCP Port 443	□
File Transfer	FTP, TCP Port 21	□
MSN Messenger	TCP Port 1863	□
Telnet Service	TCP Port 23	□
AIM	AOL Instant Messenger, TCP Port 5190	□
NetMeeting	H.323, TCP Port 1720	□
DNS	UDP Port 53	□
SNMP	UDP Port 161, 162	□
VPN-PPTP	TCP Port 1723	□
VPN-L2TP	UDP Port 1701	□
TCP	All TCP Port	□
UDP	All UDP Por	□

User Define Service	
Protocol :	Both
Port Range :	

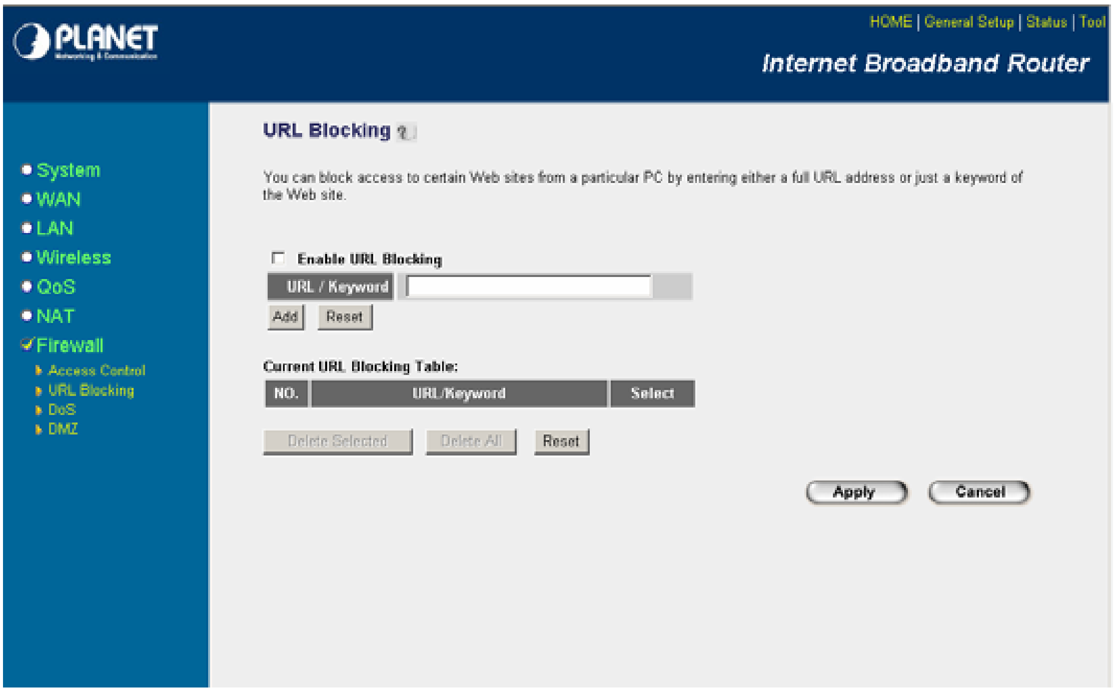
Parameters	Description
Client PC Description	The description for this client PC.
Client PC IP Addresses	Enter the IP address range that you wish to apply this Access Control rule. You can select a range of users simply by inputting the starting users’ IP address and the last user’s IP address in the appropriate boxes. If you want to select only one user, just input the user’s IP address in both boxes.

	Note: You need to give your LAN PC clients a fixed/static IP address for the Access Control rule to work properly.
Client PC Service	You can block the clients from accessing some Internet services by checking the services you want to block.
Protocol	This allows you to select **UDP**, **TCP** or **Both** protocol types.
Port Range	You can assign up to five port ranges. The router will block clients from accessing Internet services that use these ports.
Add	Click “Add” to save the settings.
Reset	Click “Reset” to clear all fields.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

5.7.2 URL Blocking

You can block users to access to some web sites by entering a full URL address or just keyword of the web site.



URL Blocking

You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site.

☐ Enable URL Blocking

URL / Keyword

Add Reset

Current URL Blocking Table:

NO.	URL/Keyword	Select

Delete Selected Delete All Reset

Apply Cancel

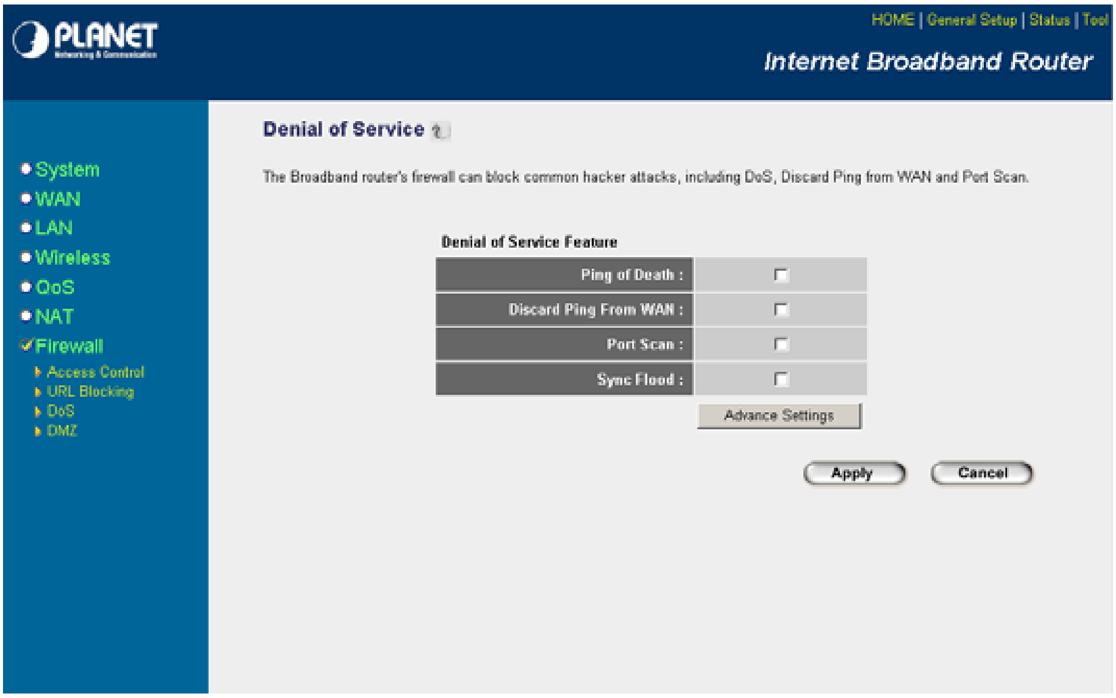
Parameters	**Description**
Enable URL Blocking	Enable/disable URL Blocking.
Add URL / Keyword	Fill in “URL / Keyword” and then click “Add”. You can enter the full URL address or the keyword of the web site you want to block. If you find any typo before adding it and want to retype again, just click "Reset" and the field will

	be cleared.
Remove URL / Keyword	If you want to remove some URL keyword from the "Current URL Blocking Table", select the URL keyword you want to remove in the table and then click "Delete Selected". If you want remove all URL keyword from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click “Reset”.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

5.7.3 DoS

WMRT-414's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur, the router can log the events.



Denial of Service

The Broadband router's firewall can block common hacker attacks, including DoS, Discard Ping from WAN and Port Scan.

Denial of Service Feature

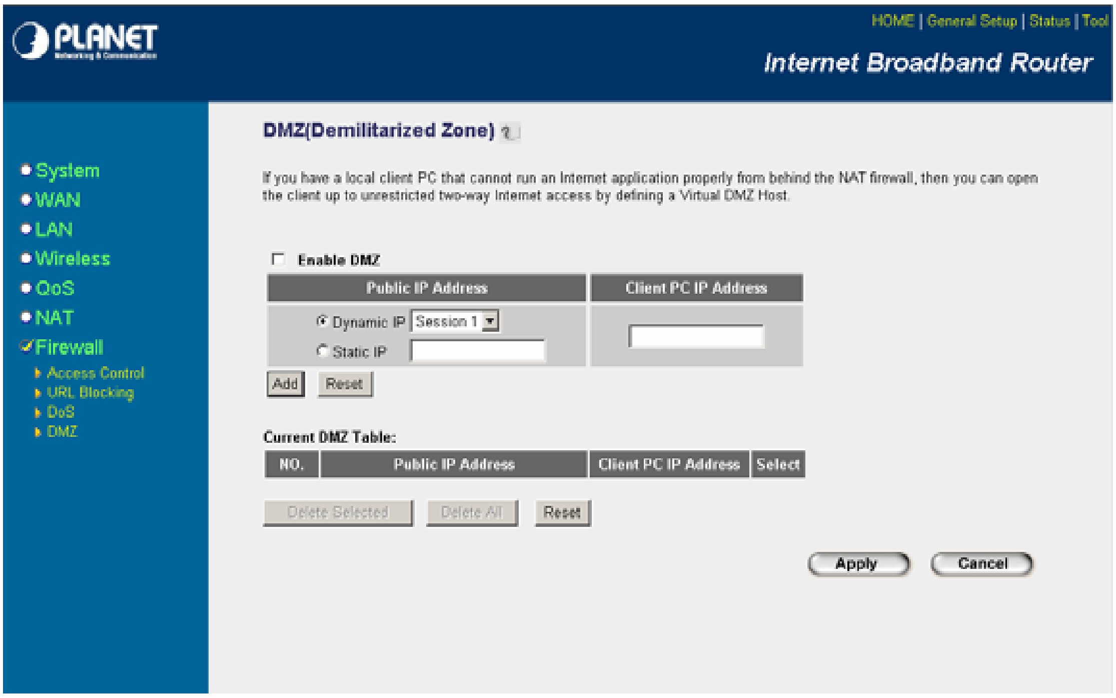
Ping of Death :	□
Discard Ping From WAN :	□
Port Scan :	□
Sync Flood :	□

Parameters	Description
Ping of Death	Protections from Ping of Death attack.
Discard Ping From WAN	The router’s WAN port will not respond to any Ping requests.
Port Scan	Protects the router from Port Scan.
Sync Flood	Protects the router from Sync Flood attack.
Advance Settings	If you want to configure the details of each setting above, click this button, and you will see the detail configure screen. Please make sure what the effect of the settings will affect before your adjustment.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

5.7.4 DMZ

If you have a local client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, you can open the client up to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets from your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) to one particular LAN client/server.


PLANET
Networking & Communication
HOME | General Setup | Status | Tool
Internet Broadband Router
System
WAN
LAN
Wireless
QoS
NAT
Firewall
Access Control
URL Blocking
DoS
DMZ

DMZ(Demilitarized Zone)

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a Virtual DMZ Host.

□ Enable DMZ

Public IP Address	Client PC IP Address
● Dynamic IP Session 1 ○ Static IP	

Current DMZ Table:

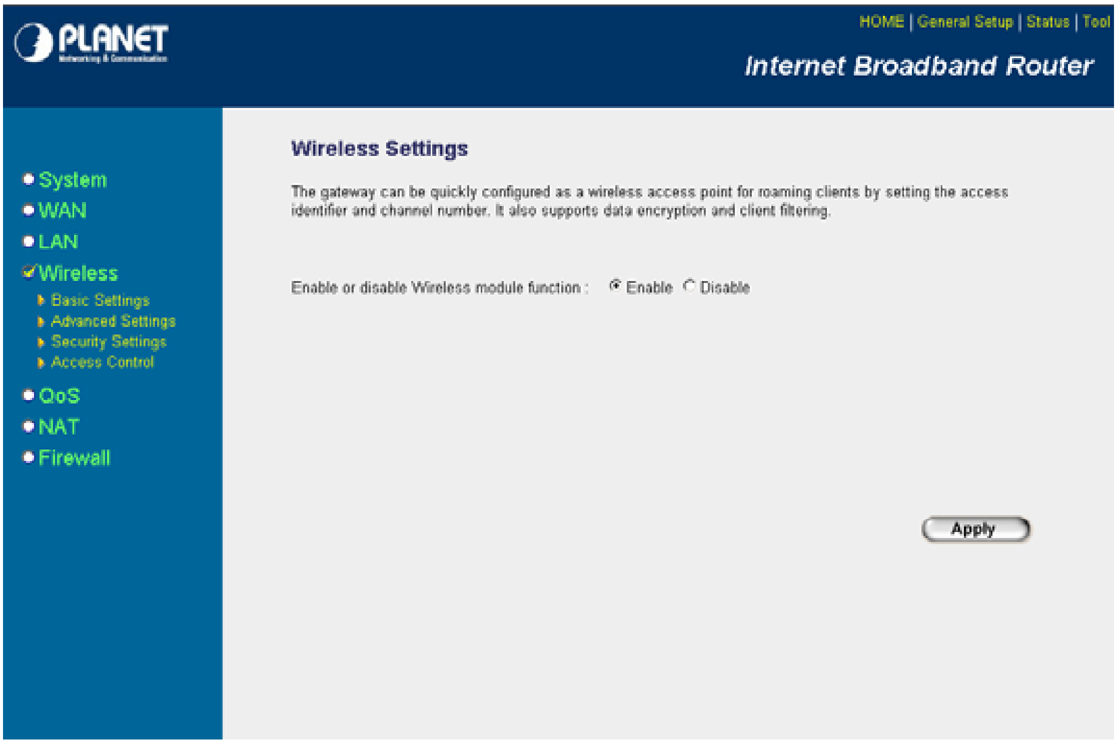
NO.	Public IP Address	Client PC IP Address	Select

Parameters	Description
Enable DMZ	Enable/disable DMZ. **Note:** If there is a conflict between the Virtual Server and the DMZ setting, the Virtual Server function will have priority over the DMZ function.
Public IP Address	The IP address of the WAN port or any other Public IP addresses given to you by your ISP.
Client PC IP Address	Input the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address above. **Note:** You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

Chapter 6 Wireless Configuration

In this chapter, you can Enable/Disable wireless function and configure the WMRT-414 work in different operating mode. Please refer to below sections to know the details configuration of each operating mode.



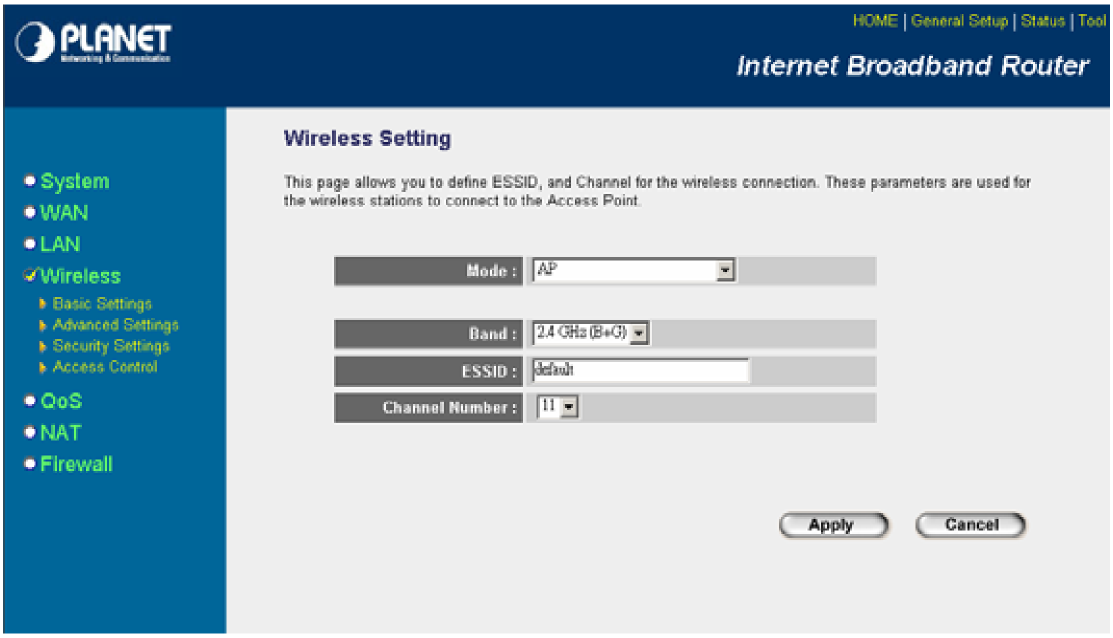
Wireless Settings

The gateway can be quickly configured as a wireless access point for roaming clients by setting the access identifier and channel number. It also supports data encryption and client filtering.

Enable or disable Wireless module function : ● Enable ○ Disable

6.1 AP Mode

This mode is set to WMRT-414 by default. It served as a transparent Media Access Control (MAC) bridge between wired and wireless network.



Wireless Setting

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode : AP

Band : 2.4 GHz (B+G)

ESSID : default

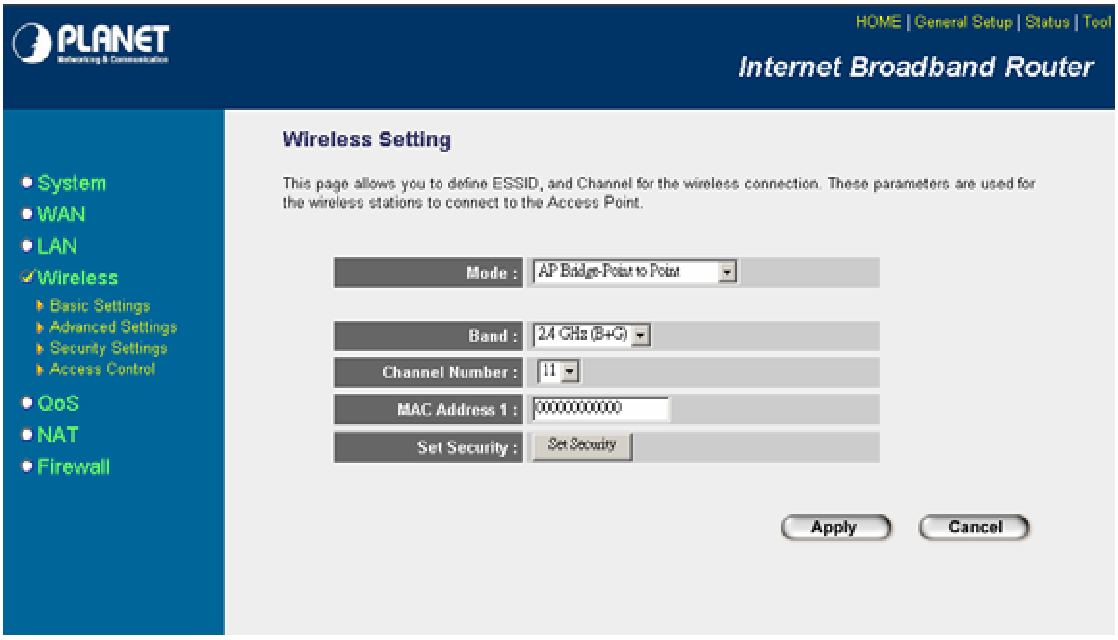
Channel Number : 11

Parameter	Description
Mode	Shows the current operation mode. You may set WMRT-414 to other operating mode by select other operating mode.
Band	**2.4GHz (B):** It forces the WMRT-414 to operate in 802.11b only. **2.4GHz (G):** It forces the WMRT-414 to operate in 802.11g only. **2.4GHz (B+G):** It allows the WMRT-414 to operate in 802.11b and 802.11g simultaneously.
ESSID	The ESSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. Please make sure that the ESSID of all stations in the same WLAN network are the same. The default value is "**default**".
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America) Channel 1-14 (Japan) Channel 1-13 (Europe)

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press "Continue" for configure other settings or "Apply" to restart WMRT-414 with new configuration.

6.2 AP Bridge - Point to Point Mode

This function allows WMRT-414 to bridge 2 wired Ethernet networks wirelessly.



Wireless Setting

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode : AP Bridge-Point to Point

Band : 2.4 GHz (B+G)

Channel Number : 11

MAC Address 1 : 000000000000

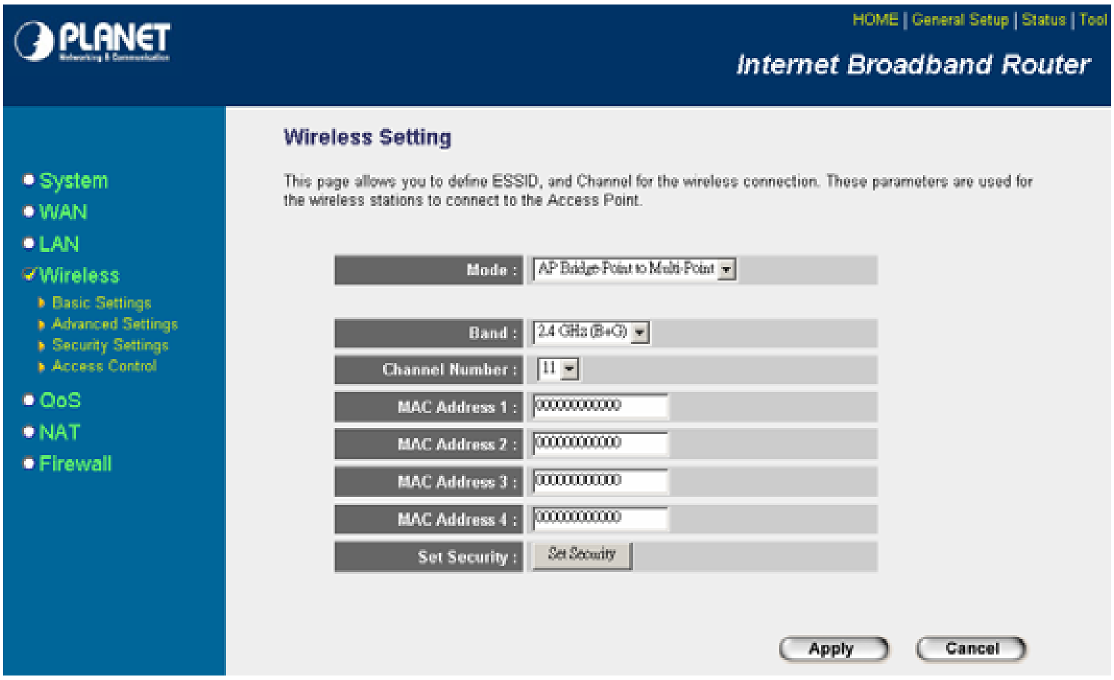
Set Security : Set Security

Parameter	Description
Mode	Shows the current operation mode. You may set WMRT-414 to other operating mode by select other operating mode.
Band	**2.4GHz (B):** It allows to select the transmit rate up to 11Mbps. **2.4GHz (G):** It allows to select the transmit rate up to 54Mbps. **2.4GHz (B+G):** It allows selecting the 802.11b and 802.11g data rates.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America) Channel 1-14 (Japan) Channel 1-13 (Europe)
MAC Address 1	Please enter the MAC Address of another WMRT-414 that this one will connect.
Set Security	IF you want to enable security to protect your wireless connection. Please press “Set Security” button and refer to section 6.5 “Security setting for bridge mode” to configure the detail settings.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

6.3 AP Bridge - Point to Multipoint Mode

This function allows WMRT-414 to bridge more than 2 wired Ethernet networks together by wireless connection.



Wireless Setting

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode : AP Bridge-Point to Multi-Point

Band : 2.4 GHz (B+G)

Channel Number : 11

MAC Address 1 : 000000000000

MAC Address 2 : 000000000000

MAC Address 3 : 000000000000

MAC Address 4 : 000000000000

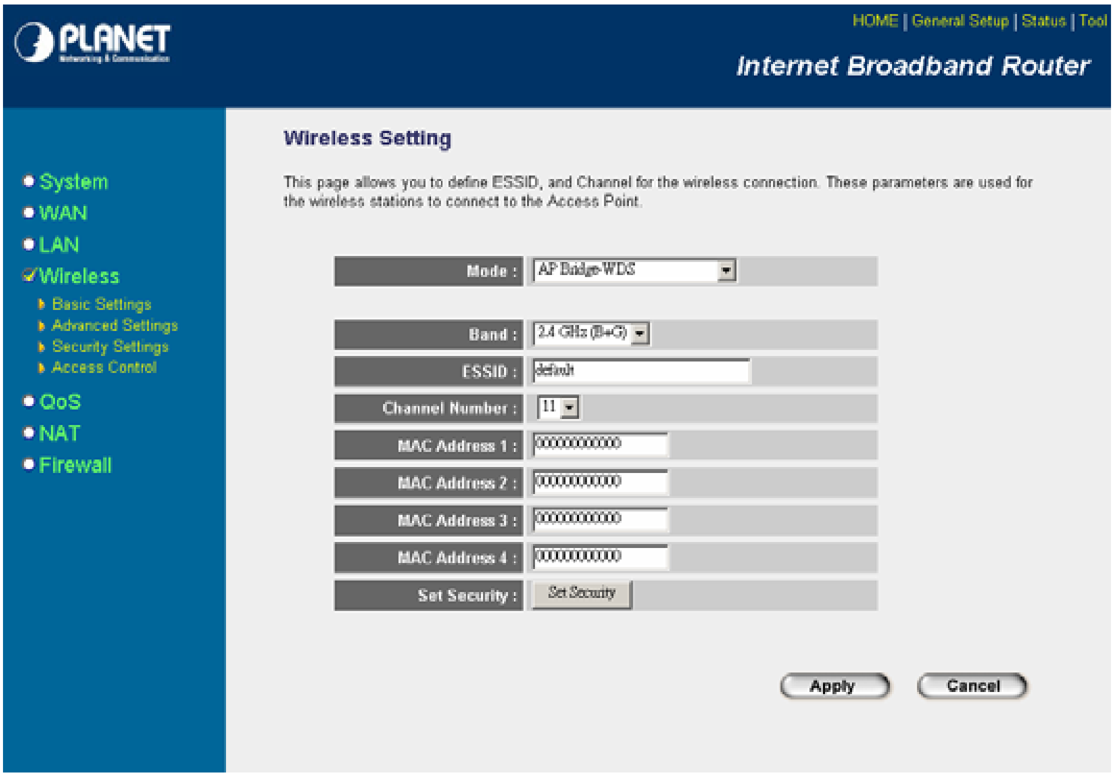
Set Security : Set Security

Parameter	Description
Mode	Shows the current operation mode. You may set WMRT-414 to other operating mode by select other operating mode.
Band	**2.4GHz (B):** It allows to select the transmit rate up to 11Mbps. **2.4GHz (G):** It allows to select the transmit rate up to 54Mbps. **2.4GHz (B+G):** It allows selecting the 802.11b and 802.11g data rates.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America) Channel 1-14 (Japan) Channel 1-13 (Europe)
MAC Address 1-4	If you want to bridge multiple WMRT-414 in this mode, you have to enter the MAC addresses of other WMRT-414 into the fields.
Set Security	IF you want to enable security to protect your wireless connection. Please press “Set Security” button and refer to section 6.5 “Security setting for bridge mode” to configure the detail settings.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

6.4 AP Bridge - WDS Mode

If you want WMRT-414 to bridge to other WMRT-414 and provide access for other wireless clients at the same time, you have to set the WMRT-414 to “AP Bridge - WDS”. Simply speaking, “AP Bridge - WDS” function is the combination of “AP mode” and “AP Bridge-Point to Multi-Point mode”.



Wireless Setting

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode :	AP Bridge-WDS
Band :	2.4 GHz (B+G)
ESSID :	default
Channel Number :	11
MAC Address 1 :	000000000000
MAC Address 2 :	000000000000
MAC Address 3 :	000000000000
MAC Address 4 :	000000000000
Set Security :	Set Security

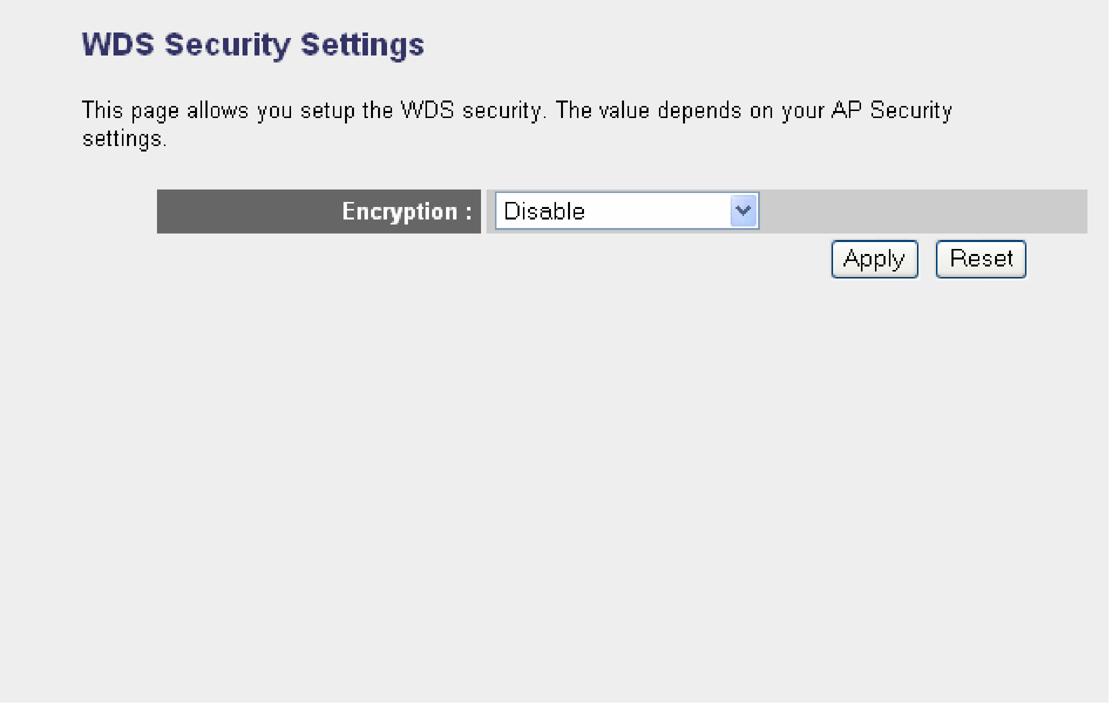
Parameter	Description
Mode	Shows the current operation mode. You may set WMRT-414 to other operating mode by select other operating mode.
Band	**2.4GHz (B):** It allows to select the transmit rate up to 11Mbps. **2.4GHz (G):** It allows to select the transmit rate up to 54Mbps. **2.4GHz (B+G):** It allows selecting the 802.11b and 802.11g data rates.
ESSID	The ESSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. Please make sure that the ESSID of all stations in the same WLAN network are the same. The default value is “**default**”.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country.

	Channel 1-11 (North America) Channel 1-14 (Japan) Channel 1-13 (Europe)
MAC Address 1-4	If you want to bridge more than two wired Ethernet networks together with wireless connection, you have to enter the MAC addresses of otherWMRT-414s that with join the bridging work into the fields.
Set Security	IF you want to enable security to protect your wireless connection. Please press "Set Security" button and refer to section "6.5 Security setting for bridge mode" to configure the detail settings.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press "Continue" for configure other settings or "Apply" to restart WMRT-414 with new configuration.

6.5 Security setting of bridge mode

In "AP Bridge-Point to Point mode", ""AP Bridge-Point to Multi-Point mode" and "AP Bridge-WDS mode", you can click "Set Security" to add encryption for the communication between the bridged access points. This can protect your wireless network.



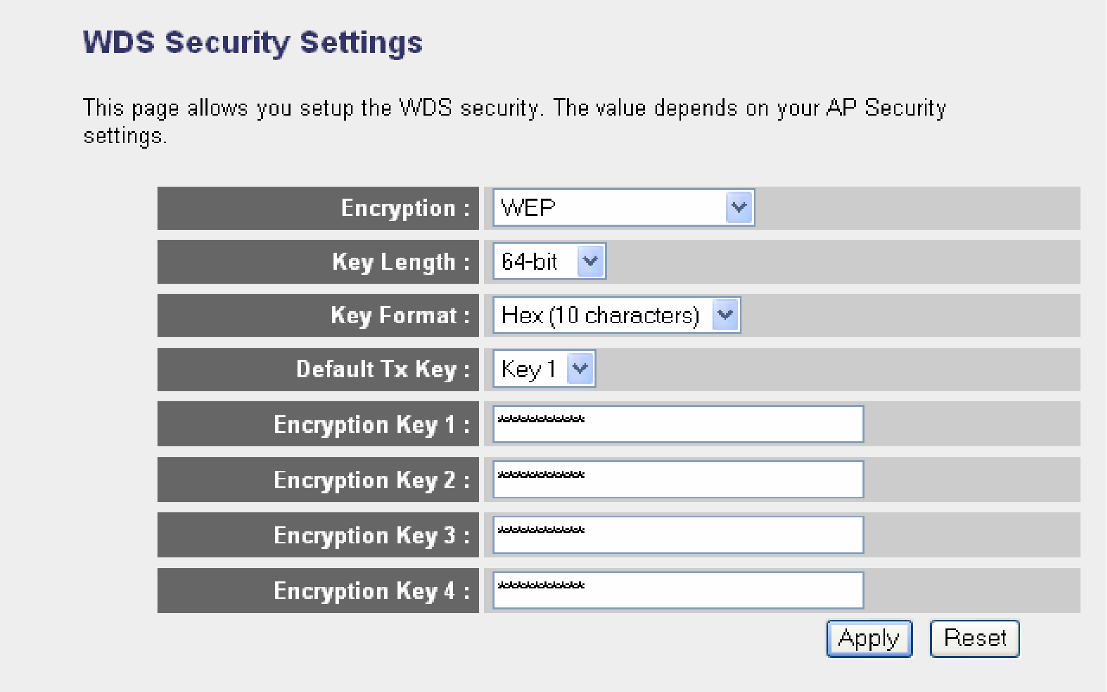
WDS Security Settings

This page allows you setup the WDS security. The value depends on your AP Security settings.

Encryption : Disable

6.5.1 WEP

When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself. You can enter four WEP keys and select one of them as default key. Then the access point will just allow the clients that with the same encryption keys connected.



WDS Security Settings

This page allows you setup the WDS security. The value depends on your AP Security settings.

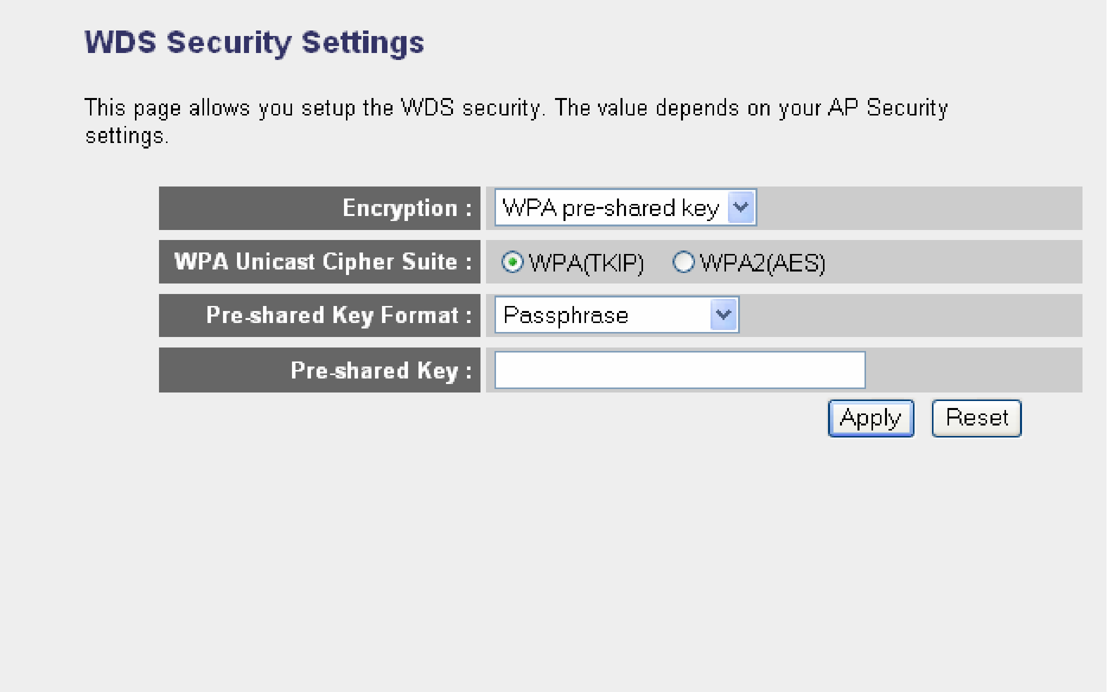
Encryption :	WEP
Key Length :	64-bit
Key Format :	Hex (10 characters)
Default Tx Key :	Key 1
Encryption Key 1 :	**********
Encryption Key 2 :	**********
Encryption Key 3 :	**********
Encryption Key 4 :	**********

Parameter	Description
Key Length	You can select the 64 or 128-bit key to encrypt transmitted data. Larger WEP key length will provide higher level of security, but the throughput will be lower.
Key Format	You may select to select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the WEP Key.
Default Tx Key	Select one of the four keys to encrypt your data. Only the key you select it in the “Default key” will take effect.
Encryption Key 1 - Key 4	The WEP keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. 64-bit WEP: input 10-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 10-digit ASCII characters as the encryption keys.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

6.5.2 WPA-PSK

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be broken by hackers. This can improve security very much.



WDS Security Settings

This page allows you setup the WDS security. The value depends on your AP Security settings.

Encryption : WPA pre-shared key

WPA Unicast Cipher Suite : ● WPA(TKIP) ○ WPA2(AES)

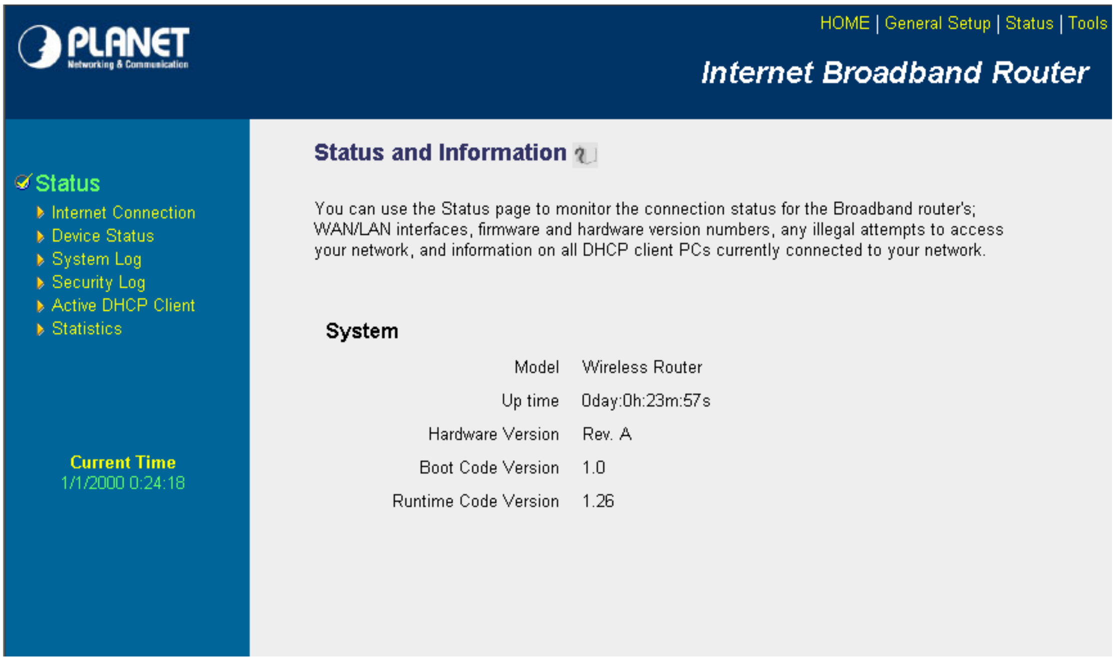
Pre-shared Key Format : Passphrase

Pre-shared Key :

Parameter		**Description**
Encryption		Please select "WPA pre-shared key" in this option.
WPA Unicast Cipher Suite	WPA (TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
	WPA2 (AES)	This use CCMP protocol to change encryption key frequently. AES can provide high-level encryption to enhance the wireless LAN security.
Pre-shared Key Format		You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the Pre-shared Key.
Pre-shared Key		The Pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill the text box by following the rules below. Hex: input 64-digit Hex values (in the "A-F", "a-f" and "0-9" range) or at least 8 character pass phrase as the pre-shared keys.

Chapter 7 Status

The Status screen allows you to monitor the current status of your router. You can use the Status page to monitor the connection status of WAN and LAN interfaces, the current firmware and hardware version numbers, any illegal attempts to access your network, and information on all DHCP client PCs currently connected to your network.



Status and Information

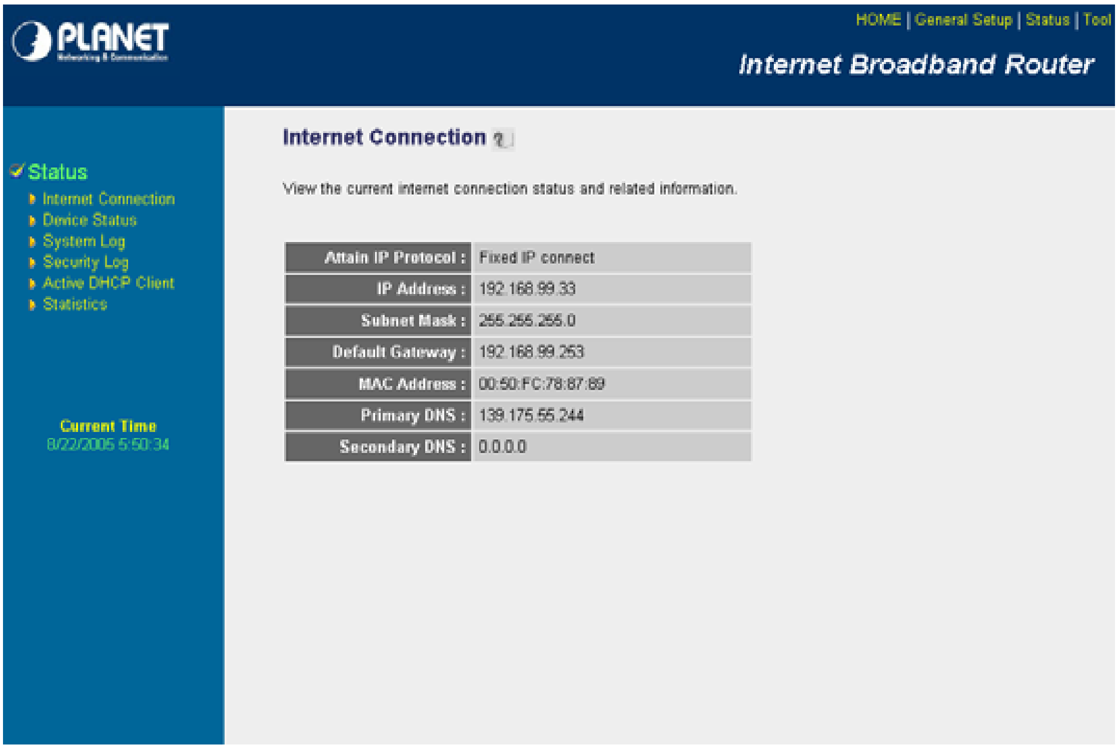
You can use the Status page to monitor the connection status for the Broadband router's; WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, and information on all DHCP client PCs currently connected to your network.

System

Model	Wireless Router
Up time	0day:0h:23m:57s
Hardware Version	Rev. A
Boot Code Version	1.0
Runtime Code Version	1.26

7.1 Internet Connection

View WMRT-414's current Internet connection status and other related information.



Current Time
8/22/2005 5:50:34

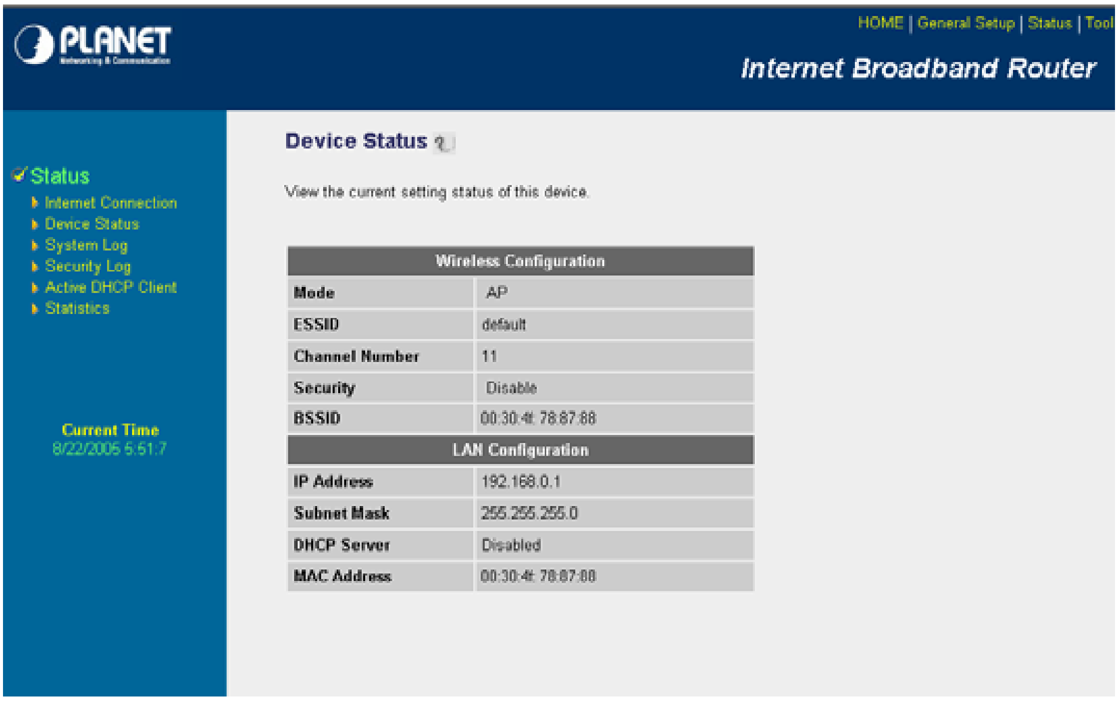
Internet Connection

View the current internet connection status and related information.

Attain IP Protocol :	Fixed IP connect
IP Address :	192.168.99.33
Subnet Mask :	255.255.255.0
Default Gateway :	192.168.99.253
MAC Address :	00:50:FC:78:87:89
Primary DNS :	139.175.55.244
Secondary DNS :	0.0.0.0

7.2 Device Status

View WMRT-414's current configuration settings. The Device Status displays the configuration settings of WLAN and LAN.



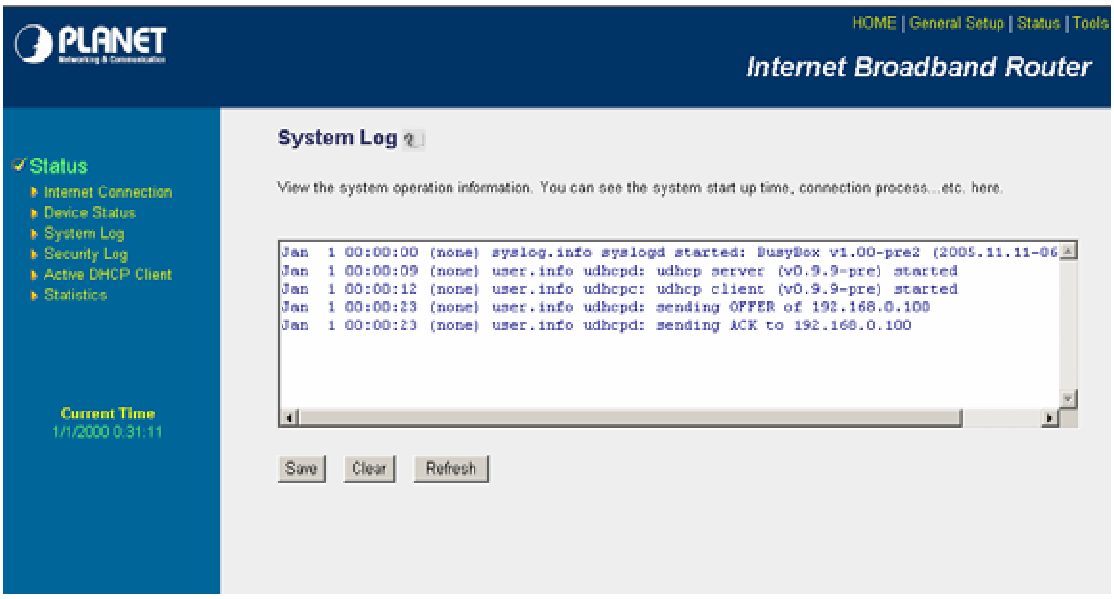
Device Status

View the current setting status of this device.

Wireless Configuration	
Mode	AP
ESSID	default
Channel Number	11
Security	Disable
BSSID	00:30:4f: 78:87:88
LAN Configuration	
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server	Disabled
MAC Address	00:30:4f: 78:87:88

7.3 System Log

This screen will show you the real-time information of WMRT-414.



System Log

View the system operation information. You can see the system start up time, connection process...etc. here.

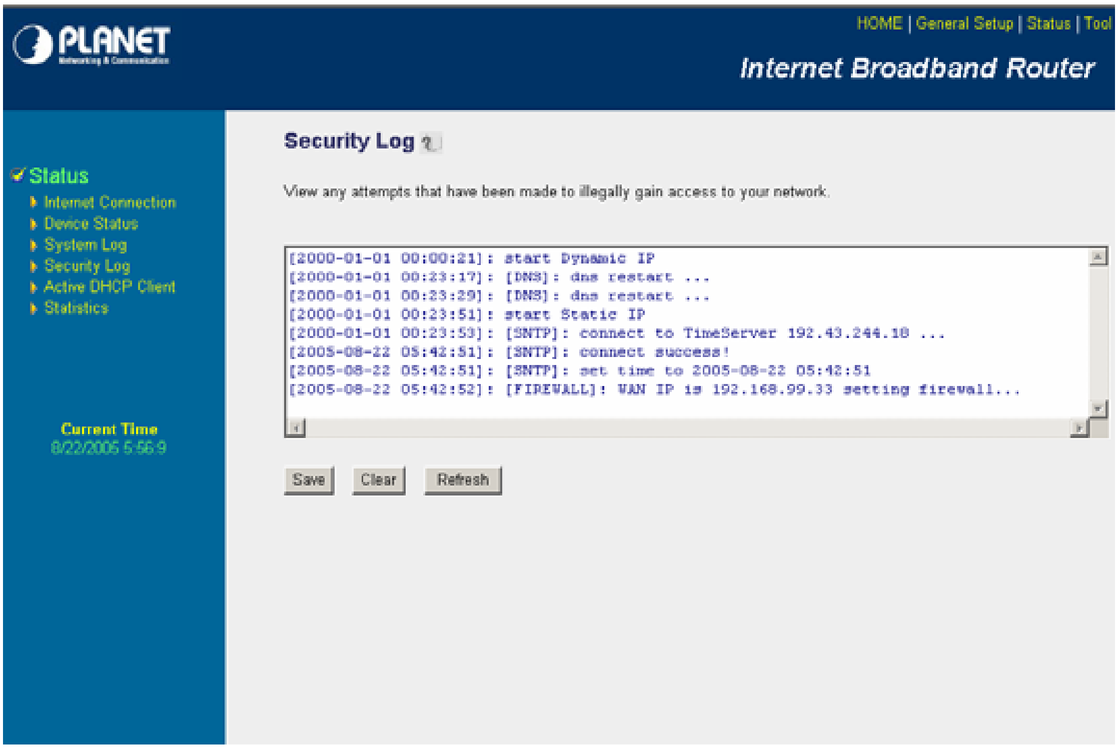
```
Jan  1 00:00:00 (none) syslog.info syslogd started: BusyBox v1.00-pre2 (2005.11.11-06
Jan  1 00:00:09 (none) user.info udhcpd: udhcp server (v0.9.9-pre) started
Jan  1 00:00:12 (none) user.info udhcpc: udhcp client (v0.9.9-pre) started
Jan  1 00:00:23 (none) user.info udhcpd: sending OFFER of 192.168.0.100
Jan  1 00:00:23 (none) user.info udhcpd: sending ACK to 192.168.0.100
```

Parameters	Description
System Log	This page shows the current system log of WMRT-414. It displays the working information about WMRT-414. About the bottoms of the page, the system log can be saved to a local file by press “Save” button. If there is too much message in this screen, please

	press “Clear” button to clear the system log . It can be refreshed to get the most updated situation by press “Refresh” button. When the system is powered down, the system log will be cleared.

7.4 Security Log

View any attempts that have been made to illegally gain access to your network.



Security Log

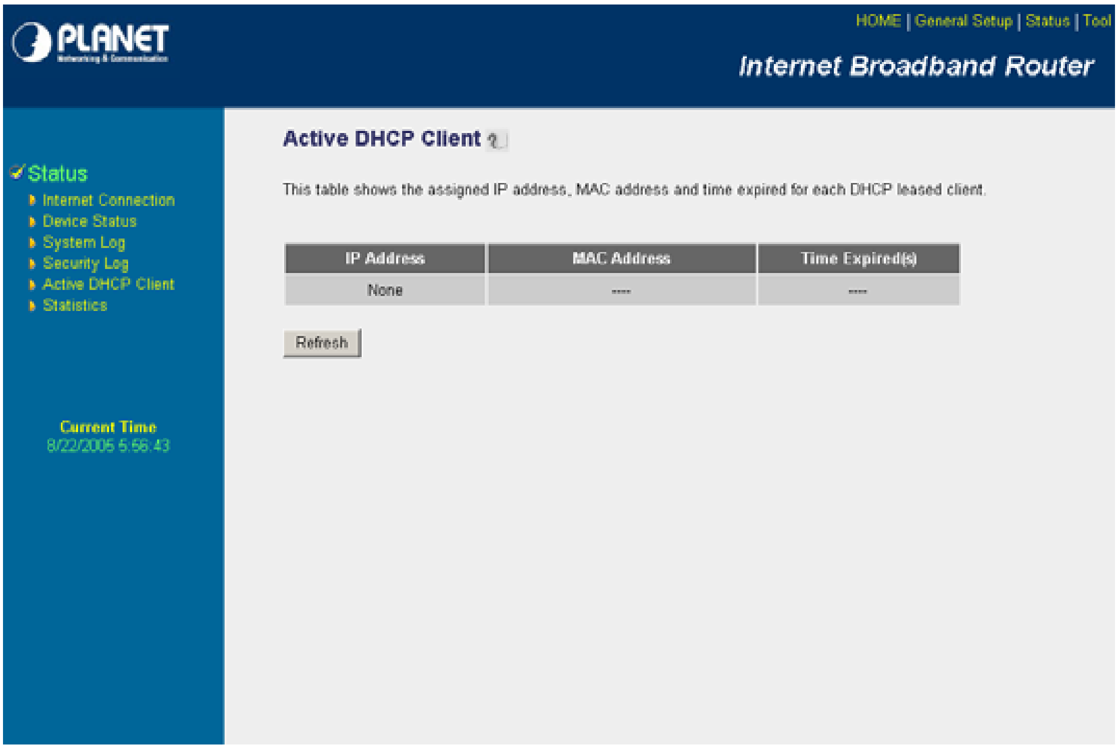
View any attempts that have been made to illegally gain access to your network.

```
[2000-01-01 00:00:21]: start Dynamic IP
[2000-01-01 00:23:17]: [DNS]: dns restart ...
[2000-01-01 00:23:29]: [DNS]: dns restart ...
[2000-01-01 00:23:51]: start Static IP
[2000-01-01 00:23:53]: [SNTP]: connect to TimeServer 192.43.244.18 ...
[2005-08-22 05:42:51]: [SNTP]: connect success!
[2005-08-22 05:42:51]: [SNTP]: set time to 2005-08-22 05:42:51
[2005-08-22 05:42:52]: [FIREWALL]: WAN IP is 192.168.99.33 setting firewall...
```

Parameters	**Description**
Security Log	This page shows the current security log of WMRT-414. It displays any illegal attempts to access your network. About the bottoms of the page, the security log can be saved to a local file by press “Save” button. If there is too much message in this screen, please press “Clear” button to clear the system log . It can be refreshed to get the most updated situation by press “Refresh” button. When the system is powered down, the security log will be cleared.

7.5 Active DHCP Client

View your client's information that is currently linked to WMRT-414's DHCP server.



Active DHCP Client

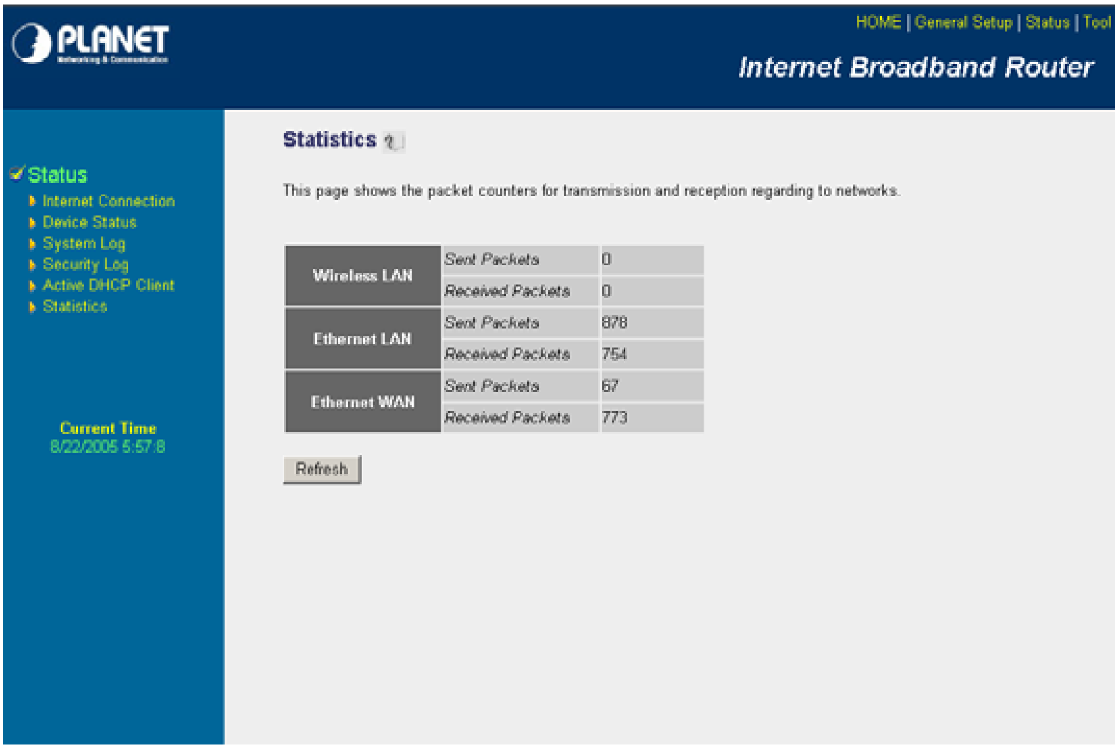
This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

IP Address	MAC Address	Time Expired(s)
None	----	----

Parameters	Description
DHCP Client Table	This page shows all the DHCP clients currently connected to your network. The “Active DHCP Client Table” displays the IP address and the MAC address and Time Expired of each Client. Use the Refresh button to get the most updated situation.

7.6 Statistics

View the statistics of packets sent and received on WLAN, LAN and WAN.



Statistics

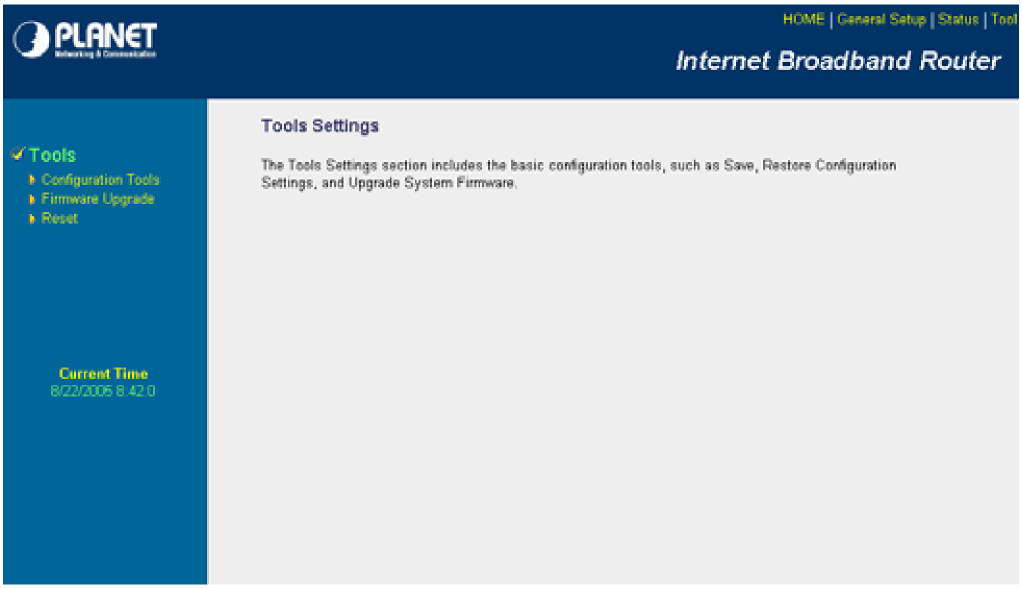
This page shows the packet counters for transmission and reception regarding to networks.

Wireless LAN	Sent Packets	0
	Received Packets	0
Ethernet LAN	Sent Packets	878
	Received Packets	754
Ethernet WAN	Sent Packets	67
	Received Packets	773

Parameters	Description
Statistics	Shows the counters of packets sent and received on WLAN, LAN and WAN.

Chapter 8 Tools

This page includes the basic configuration tools, such as Configuration Tools (save or restore configuration settings), Firmware Upgrade (upgrade system firmware) and Reset.

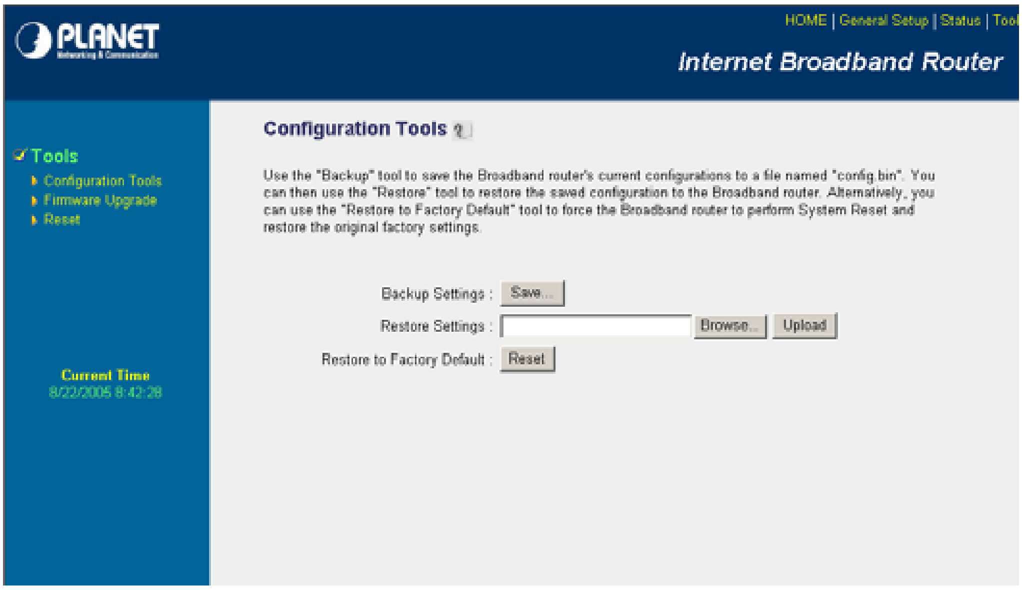

PLANET
Networking & Communication
HOME | General Setup | Status | Tool
Internet Broadband Router
Tools
Configuration Tools
Firmware Upgrade
Reset
Current Time
8/22/2005 8:42:0

Tools Settings

The Tools Settings section includes the basic configuration tools, such as Save, Restore Configuration Settings, and Upgrade System Firmware.

8.1 Configuration Tools

The Configuration Tools screen allows you to "Backup" the router's current configuration setting. Saving the configuration settings provides an added protection and convenience when problems occur and you have to reset to factory default. With the saved file, you can re-load the saved configuration into the router through the "Restore" function. If extreme problems occur you can use the "Restore to Factory Defaults" selection, this will set all configurations to its original default settings.



Configuration Tools

Use the "Backup" tool to save the Broadband router's current configurations to a file named "config.bin". You can then use the "Restore" tool to restore the saved configuration to the Broadband router. Alternatively, you can use the "Restore to Factory Default" tool to force the Broadband router to perform System Reset and restore the original factory settings.

Backup Settings :

Restore Settings :

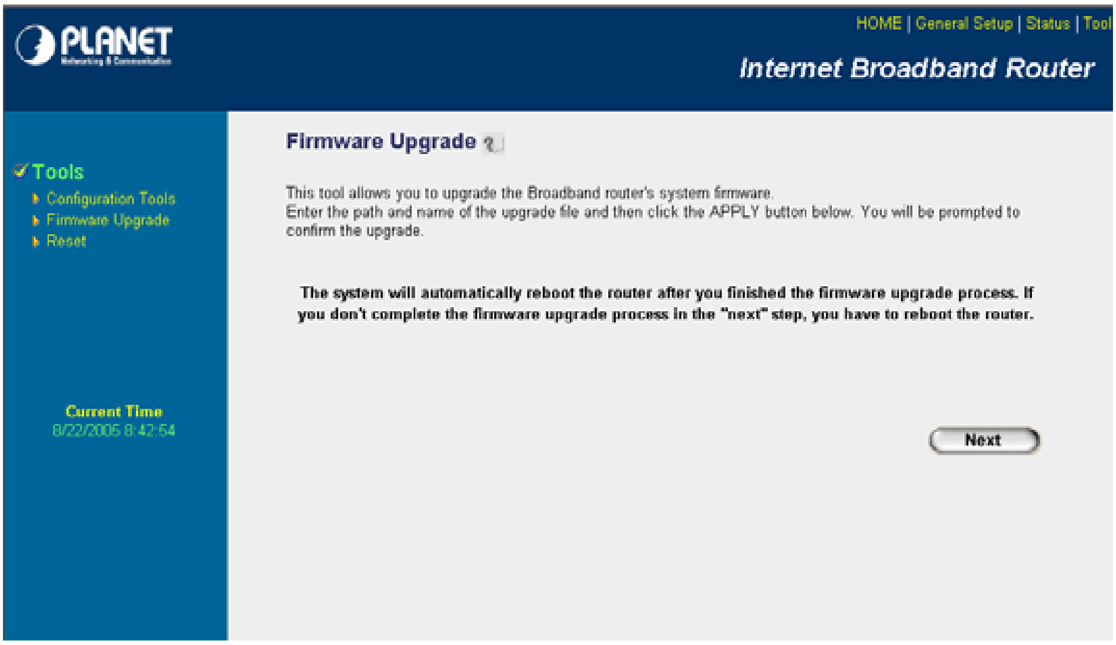
Restore to Factory Default :

Parameters	Description
Configuration Tools	Use the "**Backup**" tool to save WMRT-414 current configuration to a file named "config.bin" in your PC. You can then use the "**Restore**" tool to restore the saved configuration to WMRT-414. The "**Restore to Factory Defaults**" tool can force WMRT-414 to perform a power reset for restore it to original factory settings.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WMRT-414 with new configuration.

8.2 Firmware Upgrade

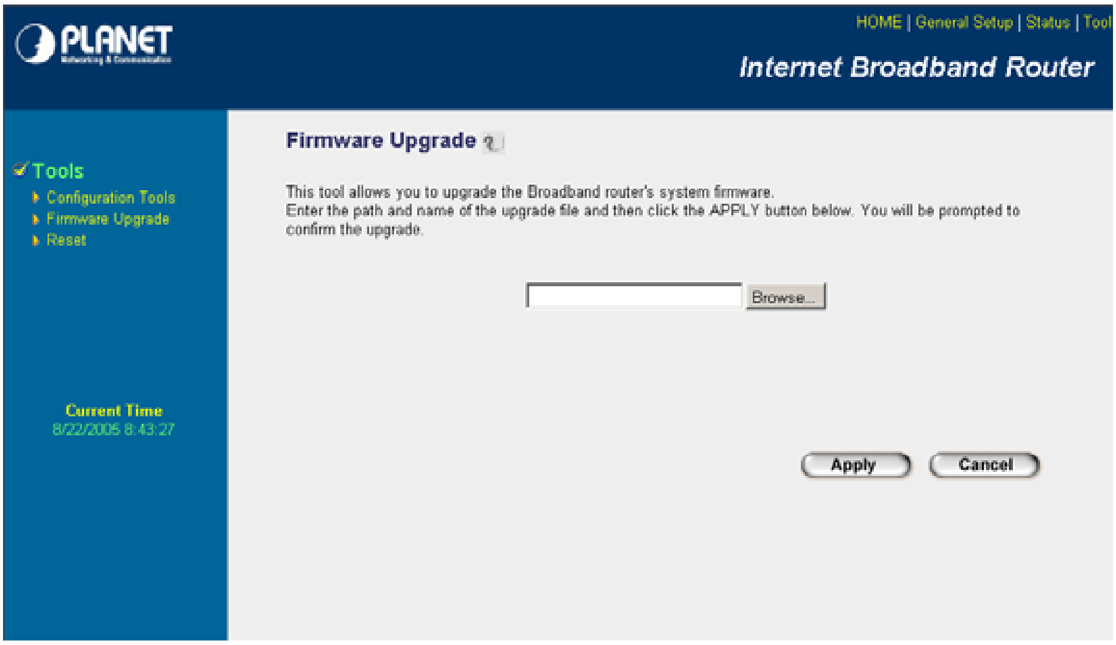
This page prompt you it allows you to upgrade the router’s firmware. Please press “Next” to continue.


PLANET
Networking & Communication
HOME | General Setup | Status | Tool
Internet Broadband Router
Tools
Configuration Tools
Firmware Upgrade
Reset
Current Time
8/22/2005 8:42:54
Next

Firmware Upgrade

This tool allows you to upgrade the Broadband router's system firmware.
Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.

The system will automatically reboot the router after you finished the firmware upgrade process. If you don't complete the firmware upgrade process in the "next" step, you have to reboot the router.



Firmware Upgrade

This tool allows you to upgrade the Broadband router's system firmware.
Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.

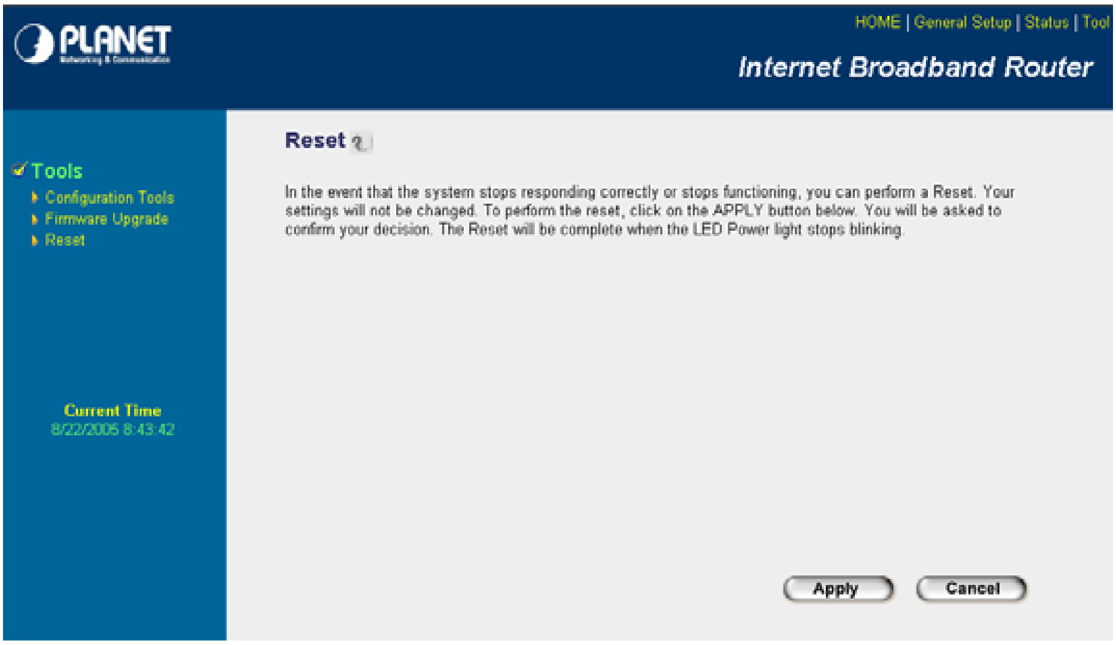
Parameters	**Description**
Firmware Upgrade	This tool allows you to upgrade WMRT-414's system firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also press the "Browse…" button to find out the firmware file on your PC.

Once you've selected the new firmware file, click "Apply" bottom to start the upgrade process. (You may have to wait a few minutes for the upgrade to complete and WMRT-414 restart). After the WMRT-414 restart, you can start using the router.

8.3 Reset

You can reset the router's system should any problem exist. The reset function is essentially

Re-boot your router.



Reset

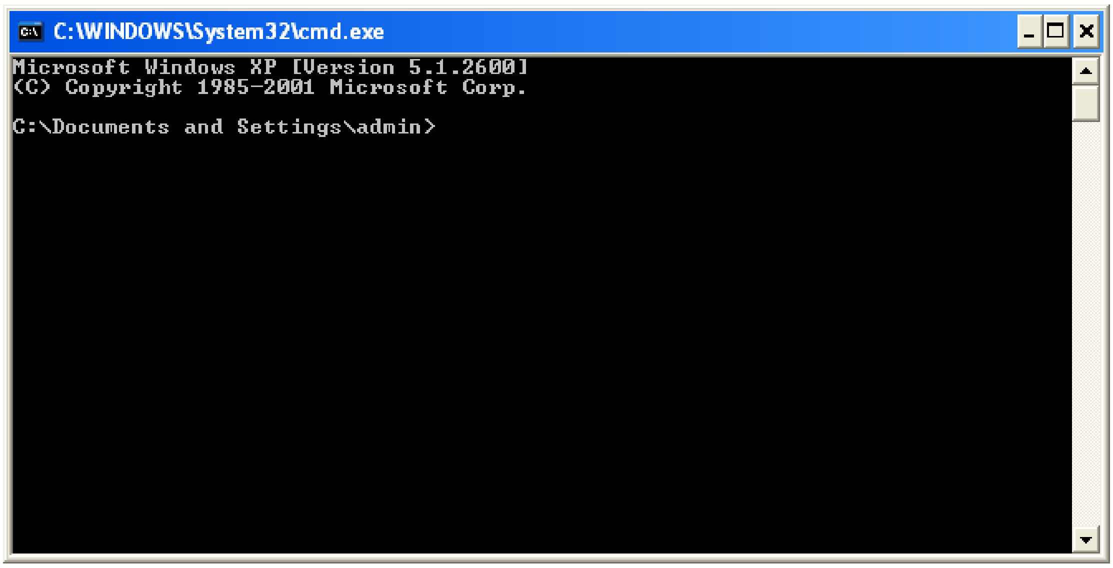
In the event that the system stops responding correctly or stops functioning, you can perform a Reset. Your settings will not be changed. To perform the reset, click on the APPLY button below. You will be asked to confirm your decision. The Reset will be complete when the LED Power light stops blinking.

Parameters	Description
Reset	In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset. **Your settings will not be changed**. To perform the reset, click on the “Apply” button. You will be asked to confirm your decision. The reset will be complete when the power light stops blinking. Once the reset process is complete you may start using the router again.

After configuration complete, please click “Apply” button, please wait for a while for the WMRT-414 restart.

Appendix A Network Adapter Information

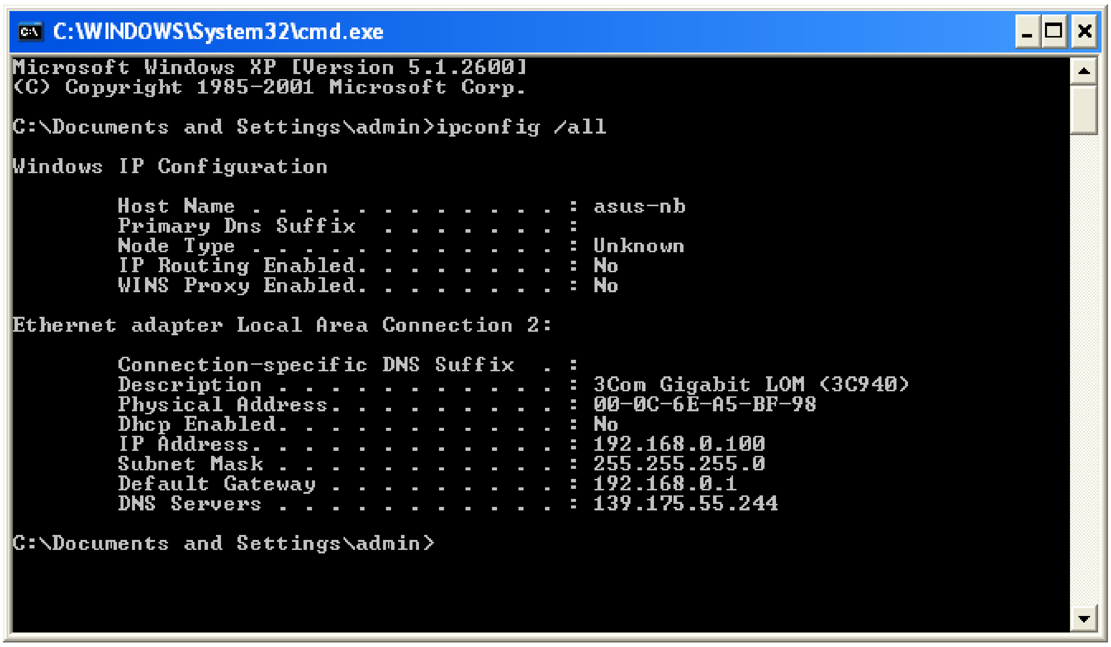
1. In Window's open the Command Prompt program.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\admin>
```

2. Type "ipconfig /all" and press "Enter" key.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\admin>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : asus-nb
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : 3Com Gigabit LOM (3C940)
        Physical Address. . . . . . . . . : 00-0C-6E-A5-BF-98
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.0.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1
        DNS Servers . . . . . . . . . . . : 139.175.55.244

C:\Documents and Settings\admin>
```

Then you can see the information of your network adapter.

Your PC's IP address is the one entitled **IP address** (192.168.0.100).

The router's IP address is the one entitled **Default Gateway** (192.168.0.1).

Your PC's MAC Address is the one entitled **Physical Address** (00-0C-6E-A5-BF-98).

Appendix B Frequently Ask Question

Q. What is MIMO?

A: **MIMO (multiple-input multiple-output)**, a technique for boosting wireless bandwidth and range by taking advantage of multiplexing. MIMO algorithms in a radio chipset send information out over two or more antennas. The radio signals reflect off objects, creating multiple paths that in conventional radios cause interference and fading. But MIMO uses these paths to carry more information, which is recombined on the receiving side by the MIMO algorithms

Many wireless-LAN vendors expect that some form of MIMO will be the basis of work just starting in the IEEE 802.11n Task Group, which is creating a specification for WLANs having at least 100M bit/sec throughput. MIMO doubles the spectral efficiency compared with that of current WLANs.

Q. Can I run an application from a remote computer over the wireless network?

A. This will depend on whether or not the application is designed to be used over a network. Consult the application’s user guide to determine if it supports operation over a network.

Q. Can I play games with other members of the wireless network?

A. Yes, as long as the game supports multiple plays over a LAN (local area network). Refer to the game’s user guide for more information.

Q. What is the IEEE 802.11g standard?

A. The IEEE 802.11g Wireless LAN standards subcommittee, which is formulating a standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

Q. What IEEE 802.11 features are supported?

A. The product supports the following IEEE 802.11 functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

Q. What is Roaming?

A. Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single Wireless Network Access Point. Before using the roaming function, the workstation must make sure that it is the same channel number with the Wireless Network Access Point of dedicated coverage area.

Q. When WMRT-414 works with WDS mode, can wireless connect to it?

A. Yes, WDS mode is work as a AP and Bridge at the same time. So the wireless client can access to WDS mode WMRT-414 without problem. When wireless client connect to the remote site via WDS mode, the performance will be 50% then access to the connected WDS mode WMRT-414. Just like connect to AP via a repeater.

Appendix C Glossary

Access Point

Access points are way stations in a wireless LAN that are connected to an Ethernet hub or server. Users can roam within the range of access points and their wireless device connections are passed from one access point to the next.

Authentication

Authentication refers to the verification of a transmitted message's integrity.

DMZ

DMZ (DeMilitarized Zone) is a part of an network that is located between a secure LAN and an insecure WAN. DMZ provides a way for some clients to have unrestricted access to the Internet.

Beacon Interval

Refers to the interval between packets sent by access points for the purposes of synchronizing wireless LANs.

DHCP

DHCP (Dynamic Host Configuration Protocol) software automatically assigns IP addresses to client stations logging onto a TCP/IP network, which eliminates the need to manually assign permanent IP addresses.

DNS

DNS stands for Domain Name System. DNS converts machine names to the IP addresses that all machines on the net have. It translates from name to address and from address to name.

Domain Name

The domain name typically refers to an Internet site address.

Filter

Filters are schemes which only allow specified data to be transmitted. For example, the router can filter specific IP addresses so that users cannot connect to those addresses.

Firewall

Firewalls are methods used to keep networks secure from malicious intruders and unauthorized access. Firewalls use filters to prevent unwanted packets from being transmitted. Firewalls are typically used to provide secure access to the Internet while keeping an organization's public Web server separate from the internal LAN.

Firmware

Firmware refers to memory chips that retain their content without electrical power (for example, BIOS ROM). The router firmware stores settings made in the interface.

Fragmentation

Refers to the breaking up of data packets during transmission.

FTP

FTP (File Transfer Protocol) is used to transfer files over a TCP/IP network, and is typically used for transferring large files or uploading the HTML pages for a Web site to the Web server.

Gateway

Gateways are computers that convert protocols enabling different networks, applications, and operating systems to exchange information.

Host Name

The name given to a computer or client station that acts as a source for information on the network.

HTTP

HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTP establishes a connection with a Web server and transmits HTML pages to client browser (for example Windows IE). HTTP addresses all begin with the prefix 'http://' prefix (for example, *http://www.yahoo.com*).

ICMP

ICMP (Internet Control Message Protocol) is a TCP/IP protocol used to send error and control messages over the LAN (for example, it is used by the router to notify a message sender that the destination node is not available).

IP

IP (Internet Protocol) is the protocol in the TCP/IP communications protocol suite that contains a network address and allows messages to be routed to a different network or subnet. However, IP does not ensure delivery of a complete message—TCP provides the function of ensuring delivery.

IP Address

The IP (Internet Protocol) address refers to the address of a computer attached to a TCP/IP network. Every client and server station must have a unique IP address. Clients are assigned either a permanent address or have one dynamically assigned to them via DHCP. IP addresses are written as four sets of numbers separated by periods (for example, 211.23.181.189).

ISP

An ISP is an organization providing Internet access service via modems, ISDN (Integrated Services Digital Network), and private lines.

LAN

LANs (Local Area Networks) are networks that serve users within specific geographical areas, such as in a company building. LANs are comprised of servers, workstations, a network operating system, and communications links such as the router.

MAC Address

A MAC address is a unique serial number burned into hardware adapters, giving the adapter a unique identification.

Metric

A number that indicates how long a packet takes to get to its destination.

MTU

MTU (Maximum Transmission/Transfer Unit) is the largest packet size that can be sent over a network.

Messages larger than the MTU are divided into smaller packets.

NAT

NAT (Network Address Translation - also known as IP masquerading) enables an organization to present itself to the Internet with one address. NAT converts the address of each LAN node into one IP address for the Internet (and vice versa). NAT also provides a certain amount of security by acting as a firewall by keeping individual IP addresses hidden from the WAN.

(Network) Administrator

The network administrator is the person who manages the LAN within an organization. The administrator's job includes ensuring network security, keeping software, hardware, and firmware up-to-date, and keeping track of network activity.

NTP

NTP (Network Time Protocol) is used to synchronize the real-time clock in a computer. Internet primary and secondary servers synchronize to Coordinated Universal Time (UTC).

Packet

A packet is a portion of data that is transmitted in network communications. Packets are also sometimes called frames and datagrams. Packets contain not only data, but also the destination IP address.

Ping

Ping (Packet Internet Groper) is a utility used to find out if a particular IP address is present online, and is usually used by networks for debugging.

Port

Ports are the communications pathways in and out of computers and network devices (routers and switches). Most PCs have serial and parallel ports, which are external sockets for connecting devices such as printers, modems, and mice. All network adapters use ports to connect to the LAN. Ports are typically numbered.

PPPoE

PPPoE (Point-to-Point Protocol Over Ethernet) is used for running PPP protocol (normally used for dial-up Internet connections) over an Ethernet.

Preamble

Preamble refers to the length of a CRC (Cyclic Redundancy Check) block that monitors communications between roaming wireless enabled devices and access points.

Protocol

A protocol is a rule that governs the communication of data.

RIP

RIP (Routing Information Protocol) is a routing protocol that is integrated in the TCP/IP protocol. RIP finds a route that is based on the smallest number of hops between the source of a packet and its destination.

RTS

RTS (Request To Send) is a signal sent from the transmitting station to the receiving station requesting permission to transmit data.

Server

Servers are typically powerful and fast machines that store programs and data. The programs and data are shared by client machines (workstations) on the network.

SMTP

SMTP (Simple Mail Transfer Protocol) is the standard Internet e-mail protocol. SMTP is a TCP/IP protocol defining message format and includes a message transfer agent that stores and forwards mail.

SNMP

SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol. SNMP hardware or software components transmit network device activity data to the workstation used to oversee the network.

SSID

SSID (Service Set Identifier) is a security measure used in WLANs. The SSID is a unique identifier attached to packets sent over WLANs. This identifier emulates a password when a wireless device attempts communication on the WLAN. Because an SSID distinguishes WLANS from each other, access points and wireless devices trying to connect to a WLAN must use the same SSID.

Subnet Mask

Subnet Masks are used by IP protocol to direct messages into a specified network segment (i.e., subnet). A subnet mask is stored in the client machine, server or router and is compared with an incoming IP address to determine whether to accept or reject the packet.

SysLog Server

A SysLog server monitors incoming Syslog messages and decodes the messages for logging purposes.

TCP

(Transmission Control Protocol) is the transport protocol in TCP/IP that ensures messages over the network are transmitted accurately and completely.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the main Internet communications protocol. The TCP part ensures that data is completely sent and received at the other end. Another part of the TCP/IP protocol set is UDP, which is used to send data when accuracy and guaranteed packet delivery are not as important (for example, in realtime video and audio transmission).

The IP component of TCP/IP provides data routability, meaning that data packets contain the destination station and network addresses, enabling TCP/IP messages to be sent to multiple networks within the LAN or in the WAN.

Telnet

Telnet is a terminal emulation protocol commonly used on the Internet and TCP- or IP-based networks. Telnet is used for connecting to remote devices and running programs. Telnet is an integral component of the TCP/IP communications protocol.

UDP

(User Datagram Protocol) is a protocol within TCP/IP that is used to transport information when accurate delivery isn't necessary (for example, real-time video and audio where packets can be dumped as there is no time for retransmitting the data).

Virtual Servers

Virtual servers are client servers (such as Web servers) that share resources with other virtual servers (i.e., it is not a dedicated server).

WEP

WEP (Wired Equivalent Privacy) is the de facto security protocol for wireless LANs, providing the "equivalent" security available in hardwired networks.

Wireless LAN

Wireless LANs (WLANs) are local area networks that use wireless communications for transmitting data. Transmissions are usually in the 2.4 GHz band. WLAN devices do not need to be lined up for communications like infrared devices. WLAN devices use access points which are connected to the wired LAN and provide connectivity to the LAN. The radio frequency of WLAN devices is strong enough to be transmitted through non-metal walls and objects, and can cover an area up to a thousand feet. Laptops and notebooks use wireless LAN PCMCIA cards while PCs use plug-in cards to access the WLAN.

WLAN

WLANs (Wireless LANs) are local area networks that use wireless communications for transmitting data. Transmissions are usually in the 2.4 GHz band. WLAN devices do not need to be lined up for communications like infrared devices. WLAN devices use access points which are connected to the wired LAN and provide connectivity to the LAN. The radio frequency of WLAN devices is strong enough to be transmitted through non-metal walls and objects, and can cover an area up to a thousand feet. Laptops and notebooks use wireless LAN PCMCIA cards while PCs use plug-in cards to access the WLAN.

WAN

WAN (Wide Area Network) is a communications network that covers a wide geographic area such as a country (contrasted with a LAN, which covers a small area such as a company building).